

RISK-AWARE ADAPTIVE SECURITY MANAGEMENT FOR EDGE-ENABLED IOMT

S. Mary Helan Felista¹, M. Ganaga Durga²

¹Research 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

²Research Supervisor, Assistant Professor, Department of Computer Applications, Sri Meenakshi Govt. Arts College for Women (Autonomous), Madurai. E-mail: mgdurga@yahoo.com

Abstract—Fixed security measures are inadequate for constantly shifting security conditions due to the growing deployment of Internet of Medical Things (IoMT) devices in healthcare settings, which creates a variety of security threats and resource restrictions. For edge-enabled IoMT, this study suggests a Risk-Aware Adaptive Security Management (RAASM) system that dynamically chooses security measures based on the evaluated security risk. By associating the computed risk score with suitable security measures, the suggested framework expands upon the EISRA risk assessment methodology. While moderate, high, and critical conditions activate increasingly robust security safeguards, low-risk scenarios use simple authentication and integrity techniques. To assess the suggested framework utilizing various IoMT device populations, edge-node topologies, assault scenarios, and attack intensities, a Python-based simulation is created. The evaluation evaluates security effectiveness and system performance utilizing risk score, attack detection rate, authentication success, latency, throughput, packet delivery ratio, CPU use, memory utilization, and energy consumption. The efficacy of adaptive security selection under changing security settings and growing IoMT workloads is examined using the experimental data. The suggested methodology takes into account the related resource and QoS constraints while offering a risk-driven method for dynamically managing security in edge-enabled IoMT contexts.

Keywords: Internet of Medical Things, Edge Computing, Security Risk Assessment, Adaptive Security, Risk-Aware Security, IoMT Security, Quality of Service, Security Management.

1. INTRODUCTION

By linking medical sensors, wearable technology, patient monitoring systems, gateways, and healthcare services, the Internet of Medical Things (IoMT) has grown to be a significant part of contemporary healthcare. IoMT supports remote and individualized healthcare services by facilitating ongoing medical data monitoring and exchange [1]. However, the abundance of diverse and resource-constrained devices also makes healthcare settings more vulnerable to security threats. [1], [2]. Denial-of-Service (DoS), Man-in-the-Middle (MitM), replay, impersonation, and data manipulation attacks are just a few of the security risks that IoMT devices and their edge networks are susceptible to. Healthcare information's availability, confidentiality, and integrity may be impacted by these risks [1], [2]. In order to safeguard IoMT environments, authentication, encryption, access control, and intrusion detection systems have been extensively studied [2], [3]. IoMT devices have different security requirements. Criticality, vulnerability, computational power, and network exposure can vary among medical equipment [2]. Furthermore, the quantity of linked devices and the severity of attacks might alter the security state of an IoMT system. Consequently, using a static security strategy across all IoMT devices could lead to wasteful resource usage or insufficient defense in the face of evolving threats. [2], [4].

Edge computing offers a chance to conduct security-related tasks nearer to IoMT devices. Processing at the edge can enable quicker security evaluations and responses, while lessening reliance on centralized cloud solutions. Recent studies have examined security and intrusion detection strategies tailored for IoMT edge settings [5]. Although IoMT security threats, risk assessment, authentication, and edge-based protection are covered in current research, security-risk assessment and adaptive security management must be connected. A security condition's severity can be determined through risk assessment, but the knowledge gathered from this process should also be converted into a suitable security response.

This encourages a system where the degree of security protection implemented at the edge is dynamically determined by the evaluated risk. A Risk-Aware Adaptive Security Management (RAASM) framework for Edge-Enabled IoMT is proposed in this study. By classifying the existing security condition and choosing a suitable security response based on the computed risk score, the suggested method expands on the EISRA risk assessment idea. Stronger protection is applied to high-risk conditions, while light weight protection is activated as the risk level decreases.

The main contributions of this paper are:

1. An adaptive security management framework for edge-enabled IoMT that is risk-aware.
2. A risk-to-security mapping system that links suitable security measures to EISRA risk categories.
3. Dynamic security selection in response to evolving IoMT security circumstances.
4. Simulation-based evaluation under varying IoMT device populations, edge nodes, and attack intensities.
5. Security and QoS analysis employing detection rate, authentication success, latency, throughput, PDR, CPU utilization, memory utilization, and energy consumption..

The rest of the document is structured as follows: The proposed RAASM framework is described in Section 3, the implementation and simulation technique is presented in Section 4, and related work is presented in Section 2. The results are discussed in Section 5, a comparative analysis is given in Section 6, and the study is concluded in Section 7.

2. RELATED WORK

2.1 IoMT Security and Threats

This is due to the fact that medical communication networks are diverse, heterogeneous, heterogeneous, heterogeneous, and heterogeneous. Threats such unauthorized access, data interception, device impersonation, denial-of-service, and data manipulation have been recognized as significant security issues in IoMT contexts by previous research [6]. Thus, security measures like intrusion detection, access control, encryption, and authentication have been suggested to safeguard medical equipment and patient information [7]. Because different devices and services may have varying security requirements, risk assessment has also become a crucial part of IoMT security. When assessing the security state of an IoMT environment, a risk-oriented approach might take into account elements such device criticality, vulnerability, likelihood, impact, and exposure [8].

2.2 Edge-Based Security for IoMT

Edge computing can lessen reliance on centralized cloud infrastructure by bringing security and computational features closer to IoMT devices. Applications in the healthcare industry that demand prompt processing and response will find this especially helpful. The significance of taking into account both security circumstances and edge-resource limits has been highlighted by recent research on edge-based intrusion detection and security procedures for IoMT systems [9]. However, security processing at the edge also consumes computational resources. As the number of IoMT devices increases, CPU utilization, memory consumption, latency, and energy requirements may increase. Therefore, security mechanisms should consider the available edge resources when determining an appropriate protection strategy.

2.3 Adaptive Security Management

IoMT devices are often subjected to predetermined protection methods via conventional security mechanisms. These methods might not be able to react sufficiently to attack conditions that change over time. By adapting the security response to the present danger or risk scenario, adaptive security offers an option. A determined risk score can be used by a risk-aware adaptive mechanism to decide whether more robust or light security protection is needed. For example, low-risk conditions may use lightweight authentication and integrity verification, whereas high-risk conditions may activate enhanced authentication, encryption, and continuous verification.

2.4 Research Gap

IoMT security, risk assessment, edge-based protection, and adaptive security techniques have all been studied independently in the past [6]–[9]. Nonetheless, there is potential for combining these elements into a single framework where security risk directly influences the choice of edge security measures. In order to extend the EISRA risk assessment method, this study suggests a Risk-Aware Adaptive Security Management (RAASM) architecture that links the computed risk score to a suitable security response. After that, various IoMT populations, edge-node topologies, assault scenarios, and attack intensities are used to assess the framework.

3. PROPOSED RISK-AWARE ADAPTIVE SECURITY MANAGEMENT FRAMEWORK

3.1 System Architecture

By utilizing the computed security risk to dynamically choose the best security response, the suggested Risk-Aware Adaptive Security Management (RAASM) architecture expands upon the EISRA risk assessment method. The framework consists of IoMT devices, an edge gateway, risk assessment, risk classification, adaptive security selection, edge nodes, and the healthcare cloud. The main location for gathering device and security data and making adaptive security decisions is the edge gateway. The framework is designed to provide enhanced protection when the evaluated risk grows while avoiding superfluous security processing under low-risk scenarios.

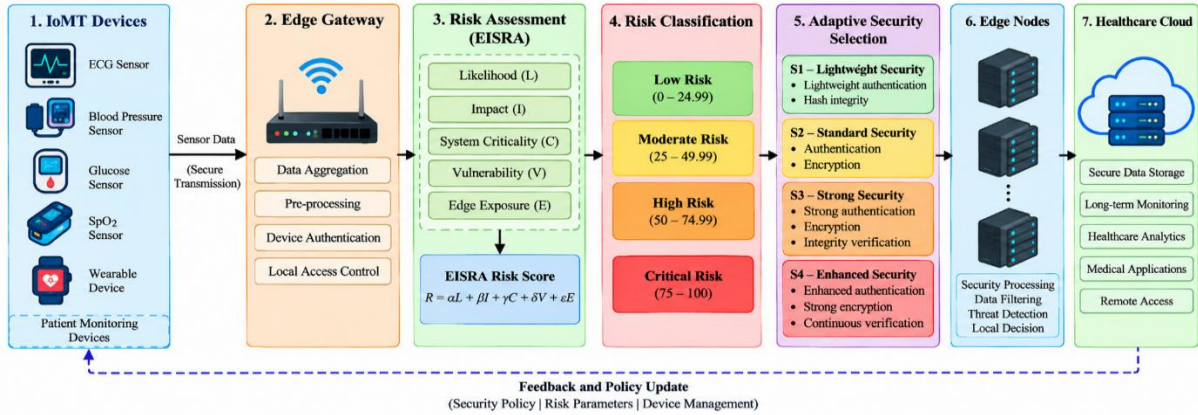


Figure 1. Proposed Risk-Aware Adaptive Security Management Architecture for Edge-Enabled IoMT

3.2 Risk Assessment

The security state of the IoMT environment is represented by the suggested framework using the EISRA risk score. The risk score is determined using likelihood, impact, device criticality, vulnerability, and edge exposure:

$$ERAS = \alpha L + \beta I + \gamma C + \delta V + \epsilon E$$

where L, I, C, V, and E represent likelihood, impact, criticality, vulnerability, and edge exposure, respectively. The weights used in the risk calculation are:

$$\alpha = 0.25, \quad \beta = 0.25, \quad \gamma = 0.15, \quad \delta = 0.15, \quad \epsilon = 0.20$$

The resulting score ranges from 0 to 100. The risk assessment considers the changing security conditions associated with IoMT devices and attack scenarios [10].

3.3 Risk Classification

The calculated ERAS value is classified into four risk levels. The classification provides the input for the adaptive security decision.

Risk Score	Risk Level	Security Response
0–24.99	Low	Lightweight authentication and integrity verification
25–49.99	Moderate	Authentication and encryption
50–74.99	High	Strong authentication, encryption, and integrity verification
75–100	Critical	Enhanced authentication, encryption, and continuous verification

This classification enables the edge gateway to select a security response according to the current risk condition.

3.4 Adaptive Security Selection

After risk classification, the edge gateway picks the corresponding security level. Under low-risk conditions, lightweight security methods are employed to reduce unnecessary processing. Additional security measures are triggered when the risk rises. The adaptive process can be represented as: $\text{Security Level} = f(\text{ERAS})$, where the security level is determined by the calculated ERAS value. If the security condition changes, the risk score can be recalculated and the security response can be updated accordingly.

3.5 Security Management Process

The complete RAASM process consists of the following steps:

1. IoMT devices generate healthcare and security-related traffic.
2. The edge gateway collects the required security parameters.
3. The EISRA risk score is calculated.
4. The resulting score is classified as Low, Moderate, High, or Critical.
5. The corresponding security level is selected.
6. The selected security mechanism is applied at the edge.
7. Security and QoS parameters are measured.
8. The security condition is reassessed for subsequent adaptation.

This process allows security protection to respond to changing IoMT risk conditions rather than relying on a single fixed security configuration.

4. IMPLEMENTATION AND SIMULATION METHODOLOGY

4.1 Simulation Environment

A Python-based simulation is constructed to assess the proposed Risk-Aware Adaptive Security Management (RAASM) system. Heterogeneous IoMT devices, edge nodes, security events, attack scenarios, risk assessment, and adaptive security selection are all modeled in the simulation. The adaptive security choice is based on the EISRA risk score. The classified security risk response is applied at the edge level. The simulation assesses both security efficacy and system performance under different IoMT workloads.

4.2 Simulation Configuration

Various IoMT device populations and associated edge-node topologies are taken into account in the simulation. ECG, blood pressure (BP), glucose, SpO₂, and wearable devices are the five categories of medical devices that are taken into consideration. Five assault scenarios are assessed at varying attack intensities: DDoS, Man-in-the-Middle (MitM), Replay, Data Injection, and Device Impersonation.

Parameter	Configuration
Simulation environment	Python
IoMT devices	10, 25, 50, 100, 150, 200
Edge nodes	1, 1, 2, 4, 5, 8
Device types	ECG, BP, Glucose, SpO ₂ , Wearable
Attack scenarios	DDoS, MitM, Replay, Data Injection, Device Impersonation
Attack intensity	Low, Moderate, High, Very High
Risk levels	Low, Moderate, High, Critical
Simulation runs	30 per configuration
Random seed	42

4.3 Experimental Procedure

Figure 3 shows the general experimental process of the suggested RAASM architecture. IoMT devices and edge nodes are initialized by the simulation, which also creates both normal and attack traffic, determines and categorizes the security risk, chooses and implements the appropriate adaptive security mechanism, and measures security and QoS parameters. Each setup is done for 30 runs, and the average results are used for analysis.

Figure 3. Experimental Procedure of Proposed Risk-Aware Adaptive Security Management Framework.



4.4 Evaluation Metrics

The suggested security, performance is assessed. Risk score, attack detection rate, and authentication success rate are used to gauge how effective security is. Edge latency, throughput, packet delivery ratio (PDR), CPU utilization, memory utilization, and energy consumption are used to assess system performance. These measures are chosen to investigate whether adaptive security management can maintain acceptable edge-system performance while responding to evolving risk conditions [11].

5. RESULTS AND DISCUSSION

5.1 Risk-Based Adaptive Security Performance

The security level is dynamically chosen by the suggested RAASM architecture based on the EISRA risk score. Four security levels are taken into account in the simulation: S1 for low risk, S2 for moderate risk, S3 for high risk, and S4 for critical danger. The framework initiates more robust security processing as the security risk rises.

Table 3. Risk-Based Adaptive Security Selection

Risk Level	Risk Score	Security Level	Security Response
Low	0–24.99	S1	Lightweight authentication + hash integrity
Moderate	25–49.99	S2	Standard authentication + encryption
High	50–74.99	S3	Strong authentication + encryption + integrity verification
Critical	75–100	S4	Enhanced authentication + strong encryption + continuous verification

The adaptive selection allows the security mechanism to respond according to the assessed risk rather than applying the same protection level to all IoMT devices.

5.2 Scalability Analysis

The scalability experiment was conducted using **10, 25, 50, 100, 150, and 200 IoMT devices** with 1, 1, 2, 4, 5, and 8 edge nodes, respectively. Each configuration was evaluated over 30 simulation runs.

Table 4. Scalability Results

IoT Devices	Edge Nodes	Risk Score	Security Level	Latency (ms)	Throughput (Mbps)	PDR (%)	CPU (%)	Memory (%)	Energy (J)	Detection (%)	Authentication (%)
10	1	67.736	S3	16.779	10.650	95.54	38.769	29.460	15.450	95.38	98.79
25	1	68.466	S3	17.983	13.125	95.15	40.849	30.552	20.749	95.49	98.81
50	2	69.651	S3	19.687	17.500	94.60	44.271	32.168	29.535	95.62	98.83
100	4	72.172	S3	23.112	26.250	93.50	51.324	35.621	47.226	95.96	98.89
150	5	74.769	S3	26.720	34.750	92.30	58.090	38.946	64.868	96.21	98.93
200	8	77.262	S4	29.892	43.750	91.30	65.113	42.325	82.517	96.51	98.98

The average risk score rises from 67.736 for 10 devices to 77.262 for 200 devices, according to the statistics. At 200 devices, S3 security gives way to S4 security due to the growing number of devices. Throughput rises from 10.650 Mbps to 43.750 Mbps, while edge latency rises from 16.779 ms to 29.892 ms. As the IoMT population grows, PDR drops from 95.54% to 91.30%. Memory consumption rises from 29.460% to 42.325%, while CPU utilization rises from 38.769% to 65.113%. Additionally, energy usage rises from 15.450 J to 82.517 J. Across all setups, the detection rate stays above 95% and the authentication success rate is above 98%.

5.3 Attack-Intensity Analysis

The proposed mechanism was further evaluated under four attack-intensity levels: Low, Moderate, High, and Very High.

Table 5. Attack-Intensity Results

Attack Intensity	Risk Score	Detection (%)	Authentication (%)	Latency (ms)	CPU (%)	Energy (J)
Low	62.037	95.50	98.88	20.311	44.081	40.942
Moderate	68.419	95.21	98.79	21.412	46.685	42.326
High	74.973	95.92	98.86	23.015	51.460	44.179
Very High	81.275	96.81	98.97	24.711	56.719	46.117

According to the findings, the danger score rises to 81.275 with Very High assault intensity from 62.037 under Low attack intensity. Stronger, Adaptive Risk Risk Risk Risk Risk Risk Risk Risk Risk Risk Risk Risk Risk Risk Risk Risk increases. The average detection rate is 96.81% and the authentication success rate is 98.97% at Very High attack intensity. Latency increases from 20.311 ms to 24.711 ms, while CPU utilization climbs from 44.081% to 56.719%. As assault intensity rises, energy consumption rises from 40.942 J to 46.117 J.

5.4 Security and QoS Discussion

In accordance with the recommended security security security, the simulation, it shows that the calculated danger. Stronger security protection is engaged when the corresponding risk threshold is met, and the risk score rises with rising IoMT populations and attack intensities. The scalability results demonstrate that latency, CPU utilization, memory utilization, and energy consumption all rise with the number of IoMT devices. The security measures, which show detection rates above 95% and authentication success above 98%, are comparatively consistent at the same time. The attack-intensity experiment further demonstrates that a higher assault intensity raises the security risk and necessitates more processing. The resultant increase in latency, CPU utilization, and energy consumption represents the additional security processing associated with higher-risk scenarios. Overall, the findings show how the suggested risk-driven adaptive security management system works, where security protection is constantly modified in response to shifting IoMT security situations while security and QoS metrics are assessed concurrently.

6. COMPARATIVE ANALYSIS

6.1 Feature-Based Comparison

The proposed framework is based on the risk. It is based on the risk. Risk assessment, adaptive security selection, edge-based decision-making, and system performance considerations are the main areas of comparison.

Table 6. Feature-Based Comparison of IoMT Security Approaches

Feature	Fixed Security	Risk-Based Security	Adaptive Security	Proposed RAASM
IoMT security protection	✓	✓	✓	✓
Risk assessment	–	✓	✓	✓
Risk-level classification	–	✓	✓	✓
Adaptive security selection	–	Limited	✓	✓
Edge-based decision	Limited	✓	✓	✓
Attack-aware response	Limited	✓	✓	✓
Dynamic security response	–	Limited	✓	✓
QoS evaluation	Possible	Possible	Possible	✓
Resource consideration	Limited	Limited	✓	✓

The comparison reveals that while risk-based techniques take security risk into account when making decisions, traditional fixed-security approaches typically apply predefined security protection. Adaptive techniques further allow security protection to alter according to the prevailing security condition. Risk assessment, risk-level classification, adaptive security selection, and edge-based security management are all included in the suggested RAASM framework. The suggested method modifies the security response based on the determined EISRA risk score, in contrast to a fixed security configuration. The operation of this adaptive mechanism under growing IoMT device populations and assault intensities is further illustrated by the simulation results shown in Section 5.

6.2 Security and Performance Analysis

The simulation results show that the suggested technique maintains detection rates over 95% and authentication success above 98% across the investigated scaling setups. Latency, CPU usage, and energy consumption all rise in tandem with an increase in the number of devices and the severity of attacks. The framework's adaptability is demonstrated by the shift from S3 to S4 at the maximum device population. In a similar vein, when assault intensity increases, risk scores rise, necessitating more robust security measures. As a result, the suggested framework offers a way to link dynamic security management with security-risk assessment while concurrently keeping an eye on the resulting QoS and resource requirements.

7. CONCLUSION AND FUTURE WORK

A framework for Edge-Enabled IoMT called Risk-Aware Adaptive Security Management (RAASM) was presented in this study. The E security security security security security security risk is determined by using the framework. Attack-attack-attack-attack-attack-attack-attack-attack-attack-edge-edge-device device device configurations; a Python IoMT; a Python-based simulation was carried outcomes; it was carried outcomes; it was carried outcomes; it was carried outcomes; it was carried out. The framework can change security security security security performance. Future research will concentrate on creating more detailed device-specific security policies, integrating intelligent prediction of shifting security conditions, optimizing security in conjunction with QoS and energy consumption, and testing the framework with actual IoMT devices, edge hardware, and larger-scale healthcare settings.

References

- [1] M. Papaioannou, M. Karageorgou, G. Mantas, et al., “A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT),” *Transactions on Emerging Telecommunications Technologies*, vol. 33, Art. no. e4049, 2022, doi: 10.1002/ett.4049.

- [2] P. K. Sadhu, V. P. Yanambaka, A. Abdelgawad, and K. Yelamarthi, “Prospect of Internet of Medical Things: A Review on Security Requirements and Solutions,” *Sensors*, vol. 22, no. 15, Art. no. 5517, 2022, doi: 10.3390/s22155517.
- [3] H. Alsubaei, A. Abuhussein, and S. Shiva, “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.
- [4] T. Ahmed, S. M. Abdulla, M. A. E. Iderss, A. A. A. Ali, et al., “A Survey: To Govern, Protect, and Detect Security Principles on Internet of Medical Things (IoMT),” *IEEE Access*, vol. 10, pp. 124777–124791, 2022, doi: 10.1109/ACCESS.2022.3225038.
- [5] N. Nagarajan et al., “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.
- [6] M. Papaioannou, M. Karageorgou, G. Mantas, et al., “A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT),” *Transactions on Emerging Telecommunications Technologies*, vol. 33, Art. no. e4049, 2022, doi: 10.1002/ett.4049.
- [7] H. Alsubaei, A. Abuhussein, and S. Shiva, “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.
- [8] P. K. Sadhu, V. P. Yanambaka, A. Abdelgawad, and K. Yelamarthi, “Prospect of Internet of Medical Things: A Review on Security Requirements and Solutions,” *Sensors*, vol. 22, no. 15, Art. no. 5517, 2022, doi: 10.3390/s22155517.
- [9] N. Nagarajan et al., “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.
- [10] Š. Švandová and P. Smutný, “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.
- [11] N. Nagarajan, et al., “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.
