

Article

Evaluating the Cybersecurity Risks in IoMT Devices Through Hybrid Fuzzy-Based Unified Computational Framework

Khalid Alissa 

SAUDI ARAMCO Cybersecurity Chair, Networks and Communications Department, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia; kaalissa@iau.edu.sa

Abstract

The Internet of Medical Things (IoMT) has transformed healthcare through real-time patient monitoring, intelligent diagnosis, and seamless exchange of medical data. However, the increasing interconnectivity of IoMT devices has significantly expanded the cybersecurity attack surface, exposing healthcare systems to threats that may compromise patient safety, Data Confidentiality, and service availability. Existing cybersecurity risk assessment methods often face challenges in adequately capturing the ambiguity, incompleteness, and subjectivity inherent in expert-based evaluations of IoMT security risks. To address these limitations, this paper proposes a symmetric hybrid neutrosophic fuzzy-based cybersecurity risk assessment methodology for IoMT environments. The proposed framework integrates Neutrosophic Fuzzy Sets (NFSs), the Analytic Hierarchy Process (AHP), and the Simple Average Method (SAM) to model truth, indeterminacy, and falsity in expert judgments while aggregating multiple expert opinions to produce a comprehensive cybersecurity risk assessment. The framework evaluates cybersecurity risks across seven security dimensions and twenty-eight evaluation sub-factors to identify and prioritize critical IoMT vulnerabilities and risk vectors. The experimental results indicate that Data Protection Assessment is the highest-ranked cybersecurity dimension. At the final evaluation stage, the proposed approach combines normalized criterion weights with expert risk evaluations to produce a cybersecurity risk score of 0.8504, indicating high cybersecurity risk that requires priority mitigation in IoMT situations. The proposed framework is validated by comparing it to traditional multi-criteria decision-making methods and using sensitivity analysis to assess the rankings' robustness and stability under different decision scenarios and expert preference variations. Results show that the proposed method delivers consistent, accurate, and robust risk prioritization under uncertainty, supporting IoMT cybersecurity decision-making. Healthcare organizations can use the framework to identify cybersecurity threats, prioritize mitigation techniques, and strengthen IoMT systems.



Academic Editor: Sergei Odintsov

Received: 29 June 2026

Revised: 19 July 2026

Accepted: 20 July 2026

Published: 24 July 2026

Copyright: © 2026 by the author.
Licensee MDPI, Basel, Switzerland.
This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

Keywords: Internet of Medical Things; cybersecurity risk assessment; Neutrosophic Fuzzy Sets; multi-criteria decision-making; healthcare security

1. Introduction

The rapid digitalization of healthcare has led to the growth of Internet of Medical Things (IoMT), which is a dedicated ecosystem of interconnected medical devices, sensors, wearable technologies, healthcare applications, cloud platforms and communication infrastructures [1,2]. IoMT technologies facilitate real-time patient monitoring, remote diagnosis, smart healthcare delivery and personalized treatment, thereby improving healthcare

accessibility, operational efficiency and clinical outcomes. Smart medical devices have transformed the healthcare landscape, enabling better care for patients and empowering hospitals, clinics and home care environments to make data-driven decisions.

The global diffusion of IoT technologies has accelerated the worldwide deployment of IoMT systems. The number of connected IoT devices is expected to grow significantly, from around 19.8 billion in 2025 to over 40.6 billion in 2034, reflecting the rapid expansion of interconnected digital ecosystems (see Table 1) [3]. Rapid proliferation provides new opportunities for healthcare innovation but also expands the attack surface for cybersecurity. With the growing number of connected medical devices, the healthcare infrastructure becomes more vulnerable to attacks on their functionality, communication channels, software platforms and sensitive medical data.

Table 1. Number of IoT connections worldwide (2022–2034).

Year	IoT Connections (Billions)	Type
2022	13.8	Actual
2023	15.7	Actual
2024	17.7	Actual
2025	19.8	Actual
2026	22	Forecast
2027	24.2	Forecast
2028	26.5	Forecast
2029	28.8	Forecast
2030	31.2	Forecast
2031	33.5	Forecast
2032	35.9	Forecast
2033	38.2	Forecast
2034	40.6	Forecast

As per Table 1, the exponential growth indicates the growing reliance on connected devices, including IoMT systems in healthcare. Therefore, the growing network size is increasing the cybersecurity risks, making the healthcare infrastructure more vulnerable to sophisticated cyberattacks.

In contrast to conventional information systems, cybersecurity vulnerabilities in the IoMT environments may directly impact patient health and safety [4]. Critical healthcare operations often involve medical devices such as insulin pumps, infusion pumps, pacemakers, wearable health monitors, diagnostic imaging systems, and remote patient monitoring devices [5]. Any breach of these systems could result in incorrect medical readings, disruption of treatment procedures, unauthorized changes to device settings, delayed clinical decisions or even total device failure in emergency situations. Therefore, cybersecurity in IoMT is no longer an information technology issue but a patient safety and healthcare resilience issue [6].

In addition to the operational risks, privacy and data protection have become the main concerns in IoMT ecosystems. Medical devices routinely collect, process, transmit and store sensitive healthcare information, including patient medical history, physiological parameters, treatment records, medication information and diagnostic results [7,8]. Such information can be exposed to unauthorized access, tampering or theft due to weak authentication mechanisms, insecure communication protocols, outdated firmware, inadequate encryption and improper access controls. Healthcare data breaches can lead to financial loss, loss of public trust in healthcare institutions [9,10], regulatory penalties and reputational damage.

Several real-world incidents involving vulnerable medical devices and healthcare infrastructures have highlighted the growing cybersecurity challenges faced by healthcare organizations. Cyberattacks on medical devices, ransomware incidents on hospitals and unauthorized access to healthcare networks have shown that attackers increasingly exploit weaknesses within interconnected healthcare environments [11]. These events highlight

the importance of comprehensive cybersecurity risk assessment mechanisms to identify vulnerabilities, assess threats, and prioritize mitigation strategies before attacks negatively impact patient care and healthcare operations.

To address these challenges, healthcare organizations are increasingly adopting security measures such as multi-factor authentication, encryption protocols, network segmentation, intrusion detection systems, access control policies, vulnerability management frameworks, and continuous monitoring solutions [12]. However, the success of these controls hinges on the capability of decision-makers to correctly evaluate cybersecurity risks and assign resources to the most critical vulnerabilities. Therefore, cybersecurity risk assessment is a key component of IoMT secure deployment and sustainable healthcare management.

Cybersecurity risk assessment in the IoMT environment is an inherently complex multi-criteria decision-making (MCDM) problem. The security posture of a medical device depends on several interrelated factors such as device functionality, software vulnerabilities, communication security, authentication mechanisms, network exposure, Data Confidentiality, privacy compliance, incident response readiness, and operational criticality [13,14]. These factors often interact with each other and should be evaluated together to fully understand cybersecurity risks.

Deterministic models are widely used in traditional risk assessment approaches based on the assumption that information is complete, precise, and reliable. However, cybersecurity assessments in healthcare settings are inherently characterized by uncertainty, ambiguity, incomplete knowledge, subjective judgments, and inconsistent expert opinions [15]. Owing to the dynamic nature of cyber threats and continuously evolving attack techniques, security analysts often exhibit varying levels of confidence regarding threat likelihood, vulnerability severity, exploitability, and potential impacts. Consequently, conventional risk assessment models may not adequately capture the complexity and uncertainty associated with real-world cybersecurity decision-making.

To address these limitations, researchers have increasingly explored computational intelligence techniques, including Fuzzy Set theory, Intuitionistic Fuzzy Sets, interval-valued fuzzy models, probabilistic reasoning, machine learning algorithms, and hybrid decision-support systems. Among these approaches, fuzzy theory has been widely recognized for its capability to represent linguistic assessments and uncertain expert judgments [16,17]. Nevertheless, conventional fuzzy frameworks primarily address uncertainty and hesitation, while offering limited capability to explicitly model indeterminacy and conflicting information, both of which frequently arise during cybersecurity investigations.

Neutrosophic theory extends classical fuzzy paradigms by simultaneously modeling the degrees of truth, indeterminacy, and falsity [18]. This enhanced representation enables a more realistic characterization of uncertain, incomplete, inconsistent, and conflicting cybersecurity information. Consequently, integrating neutrosophic theory with fuzzy decision-making techniques provides a more robust mechanism for accommodating expert uncertainty and improving cybersecurity risk prioritization. These capabilities are particularly valuable in IoMT environments, where threat intelligence, vulnerability evidence, and security assessments are often incomplete, dynamic, or evolving [19].

Although neutrosophic fuzzy theory has gained increasing attention in MCDM because of its ability to explicitly represent truth, indeterminacy, and falsity, its application to cybersecurity risk assessment in IoMT environments remains relatively limited. Existing neutrosophic fuzzy studies have primarily focused on general decision-making applications, such as supplier selection, healthcare management, sustainable energy planning, and resource allocation, while comparatively fewer studies have addressed cybersecurity-specific problems. Moreover, the available studies generally emphasize methodological development or generic information security evaluation without considering the distinctive

characteristics of IoMT ecosystems, where resource-constrained medical devices, heterogeneous communication technologies, safety-critical operations, and continuously evolving cyber threats introduce additional uncertainty and complexity.

Furthermore, existing neutrosophic fuzzy decision-making approaches typically employ conventional aggregation or ranking mechanisms and rarely provide an integrated framework specifically tailored for IoMT cybersecurity risk assessment. In particular, limited attention has been devoted to systematically combining neutrosophic uncertainty modeling with structured criteria weighting and transparent expert opinion aggregation to prioritize cybersecurity risks in healthcare environments. These limitations indicate the need for a dedicated decision-support framework capable of not only representing uncertainty, indeterminacy, and conflicting expert knowledge but also addressing the practical requirements of cybersecurity risk assessment in IoMT systems.

These challenges have motivated the present study to propose an integrated framework combining NFS, the AHP, and the SAM for cybersecurity risk assessment in IoMT environments. The proposed framework integrates neutrosophic fuzzy reasoning with a unified computational decision-making methodology to systematically evaluate cybersecurity threats under conditions of uncertainty, ambiguity, and incomplete information. To comprehensively capture the security characteristics of IoMT ecosystems, the framework considers seven cybersecurity dimensions and twenty-eight associated evaluation sub-factors. By integrating NFS, AHP, and SAM, the proposed methodology aggregates expert judgments and derives comprehensive cybersecurity risk ratings, thereby providing an effective decision-support tool for prioritizing cybersecurity risks in IoMT environments. The major contributions of this research are summarized as follows:

- A symmetrical unified computational framework is proposed for cybersecurity risk assessment in IoMT environments operating under uncertain, ambiguous, and incomplete information conditions.
- A hybrid neutrosophic fuzzy Simple Average Method (NF-SAM) is introduced to aggregate expert opinions and derive cybersecurity risk ratings.
- The proposed framework integrates expert knowledge with uncertainty-aware computational intelligence techniques to improve decision reliability and assessment accuracy.
- Comparative analysis with existing decision-making approaches is conducted to evaluate the effectiveness and superiority of the proposed framework.
- Sensitivity analysis is performed to validate the robustness, stability, and practical applicability of the obtained cybersecurity risk rankings under varying decision scenarios.

The results of the study show that the proposed hybrid neutrosophic fuzzy framework is able to effectively capture the uncertainty and indeterminacy inherent in cybersecurity evaluations and provide consistent and reliable prioritization of cybersecurity risks. The framework helps decision makers to identify key vulnerabilities, allocate security resources more effectively, and improve the cyber resilience of IoMT ecosystems. The results also demonstrate that the addition of neutrosophic reasoning greatly improves the robustness of the assessment when compared to conventional approaches to risk assessment.

The remainder of this paper is organized as follows. Section 2 presents the literature review, discusses existing cybersecurity risk assessment methodologies for IoMT environments, and describes the proposed NF AHP-SAM, including the evaluation criteria, research methodology, computational procedures, and decision-making process. Section 3 presents the numerical analysis, cybersecurity risk assessment, and prioritization results. It also includes comparative and sensitivity analyses to evaluate the effectiveness, robustness, and stability of the proposed framework. Section 4 discusses the research findings, highlighting the key contributions, practical implications, limitations, and future research directions. Finally, Section 5 concludes the paper.

2. Materials and Methods

2.1. Pertinent Literature Reviews

The rapid development of the IoMT has revolutionized healthcare through real-time monitoring, remote diagnosis, intelligent treatment support and personalized healthcare services [19,20]. But these benefits have also resulted in a significant increase in the attack surface for cybersecurity due to the growing interconnectivity of medical devices. IoMT devices continuously exchange sensitive healthcare information and often operate in resource-constrained environments, making them vulnerable to cyber threats such as unauthorized access, malware injection, denial-of-service attacks, data tampering, device manipulation and privacy breaches [2,3]. Accordingly, cybersecurity risk assessment is an important aspect of patient safety, healthcare system reliability, and regulatory compliance.

Researchers have proposed various computational and decision-support approaches to assess cybersecurity risks in the healthcare and IoMT environments. Most existing approaches are based on fuzzy logic, MCDM, machine learning, anomaly detection techniques, trust assessment mechanisms and hybrid intelligent systems [4,5]. Although these approaches have shown promising results, many of them are still hampered by the management of ambiguity, inconsistency, missing information and indeterminacy, which are typical features of cybersecurity decision-making contexts.

Semenova et al. proposed an optimized fuzzy secure trust assessment scheme for IoMT environments [11] in 2026. They applied fuzzy inference systems and evolutionary optimization techniques to evaluate the trust levels of medical devices based on behavioral and communication signals. The experimental results showed that the accuracy of the trust evaluation was improved compared to traditional trust mechanisms. However, the study was more focused on trust computation rather than a complete cybersecurity risk assessment. Also, the study did not explicitly model indeterminate information, which is often present in dynamic healthcare environments.

The intelligent fusion framework for anomaly detection in IoMT health devices is introduced by Pastore et al. (2026) [12], which combines attack detection through XG-Boost along with LSTM autoencoders for physiological abnormalities and device faults. Their framework reached excellent detection accuracy and close to real-time performance. The study was effective for attack identification and anomaly classification, but it was mainly focused on operational threat detection rather than systematic cybersecurity risk prioritization and decision-making under uncertainty.

Jaidi and Ksibi (2025) [13] proposed an Advanced Security Scoring System (ASSS) based on the FAHP to assess security risks in connected medical devices. The framework enables ranking of IoMT devices and prioritization of mitigation strategies under uncertainty. The proposed model was able to incorporate expert judgments, but it still used only fuzzy representations and lacked mechanisms for dealing with indeterminacy and conflicting evidence among experts.

Obidallah (2025) [14] suggested a unified computational model based on Fuzzy ANP-TOPSIS methodology for assessing security risks in IoTT-based healthcare applications. This study demonstrated the applicability of fuzzy decision-making techniques for the selection of secure healthcare solutions. However, the focus was on transportation-healthcare integration, not device-level cybersecurity risk assessment in IoMT ecosystems.

Saad et al. [15] presented a cybersecurity framework based on fuzzy programming combining Fuzzy AHP, fuzzy TOPSIS and fuzzy linear programming for risk prioritization and resource allocation in healthcare systems. Their work effectively linked the evaluation of cybersecurity and the management of resources based on optimization. However, the framework was primarily concerned with uncertainty and did not explicitly represent inconsistent or indeterminate expert opinions.

A hybrid fuzzy logic and FAHP-based risk evaluation model for heterogeneous IoMT devices was proposed by Pritika et al. (2024) [16]. The framework was able to successfully identify and prioritize attack risks across different medical devices, demonstrating the usefulness of fuzzy decision-making techniques for healthcare cybersecurity. The model was efficient but limited to the representation of fuzzy uncertainty and did not consider incomplete evidence in cybersecurity.

A full review of IoT-based fuzzy systems in medical applications was given by Abdalla et al. (2024) [17]. Their survey showed the increasing impact of fuzzy logic in healthcare decision support, predictive analytics, and medical diagnosis. The study highlighted the ability of fuzzy approaches to handle uncertainty while identifying future opportunities involving artificial intelligence and generative AI. However, it also identified that most existing fuzzy-based healthcare systems cannot sufficiently address the indeterminacy and risk prioritization requirements specific to cybersecurity.

Khan and Ali (2024) [18] proposed a combined decision-making framework for assessing authentication schemes in Internet of Health Things (IoHT) systems based on Graph Theory and Matrix Approaches. Their framework had a high evaluation accuracy and provided a systematic methodology to authenticate evaluation. The model, however, was limited to authentication mechanisms and did not provide for the overall structure for cybersecurity risk evaluation.

Wagan et al. (2023) [19] presented a fuzzy-based duo-secure multimodal framework that fuses the Dynamic Fuzzy C-Means clustering and Bi-LSTM techniques for anomaly detection in IoMT environments. The model performed well in recognizing malware attacks and health-related anomalies. However, the study was on detection capabilities, not on strategic cybersecurity risk assessment and prioritization.

Khan et al. (2023) [20] introduced a privacy-preserving authentication assessment model using an AHP-TOPSIS hybrid framework to select appropriate authentication mechanisms in IoMT environments. The framework was able to evaluate authentication alternatives with multiple security features successfully. But it was limited to a specific cybersecurity domain and did not have the capability for wider risk assessment.

Overall, these studies indicate a significant advancement in the use of fuzzy logic, MCDM, machine learning and hybrid intelligence techniques in healthcare cybersecurity. But most of the existing methods are mainly focused on attack detection, trust management, authentication evaluation, or fuzzy-based uncertainty handling. Existing comprehensive cybersecurity risk assessment frameworks for IoMT devices have paid very little attention to addressing uncertainty, ambiguity, inconsistency and indeterminacy simultaneously. Table 2 presents a relative research study on representative works in the context of cybersecurity assessment, trust evaluation, anomaly detection and decision-making in IoMT scenarios.

The literature review reveals several important research gaps. First, most existing studies employ classical fuzzy systems, Fuzzy AHP or related fuzzy MCDM approaches for cybersecurity risk assessment. While these methods are effective for handling uncertainty and vagueness, they generally do not explicitly model indeterminacy, conflicting evidence, and incomplete cybersecurity information, which are common in complex and dynamic cybersecurity environments. In contrast, uncertainty-aware machine learning models and probabilistic anomaly detection techniques address uncertainty through different theoretical foundations and are therefore beyond the scope of this study. These limitations motivate the adoption of a neutrosophic fuzzy framework, which provides a more comprehensive representation of uncertainty by simultaneously capturing truth, falsity, and indeterminacy.

Second, many studies focus on specific domains of cybersecurity, e.g., evaluation of authentication, evaluation of trust, detection of anomalies or identification of attacks. Very few studies have a unified computational framework to evaluate the cybersecurity risks in

multi-dimensions of IoMT security. Third, current approaches usually depend on consistent judgments from experts and sufficient cybersecurity evidence. But in reality, healthcare cybersecurity environments are usually marked by ambiguous threat intelligence, uncertain vulnerability information, evolving attack patterns, and contradictory expert opinions. Fourth, although there is a high capacity of simultaneously representing truth, falsehood and indeterminacy, there is very little research on the integration of neutrosophic theory into cybersecurity risk assessment for IoMT systems.

To overcome these limitations, this paper proposes an integrated NF AHP-SAM for cybersecurity risk assessment of IoMT devices. The proposed framework differs from prior approaches as it simultaneously deals with uncertainty, ambiguity, inconsistency and indeterminacy by employing hybrid neutrosophic fuzzy reasoning. To provide a holistic risk assessment and prioritization, a comprehensive multi-criteria evaluation framework is developed, comprising seven cybersecurity dimensions and twenty-eight sub-factors. Moreover, the proposed NF AHP-SAM approach offers a systematic mechanism to aggregate expert judgments and generate reliable cybersecurity rankings. We then run comparative and sensitivity analyses to confirm the efficiency, robustness and practicality of the proposed framework, thus addressing the key gaps in the current literature.

Table 2. Summary of some pertinent cybersecurity risk assessment approaches for IoMT devices.

Study	Domain	Methodology	Uncertainty Handling	Indeterminacy Handling	Risk Prioritization	Comparative Analysis	Key Points
Semenova et al. (2026) [11]	IoMT Trust Assessment	Fuzzy Logic + Evolutionary Optimization	Yes	No	Partial	Yes	Focused on trust assessment only
Pastore et al. (2026) [12]	Anomaly Detection	XGBoost + LSTM Fusion	Limited	No	No	Yes	Detection-oriented framework
Jaidi and Ksibi (2025) [13]	IoMT Security Evaluation	FAHP	Yes	No	Yes	Limited	Expert dependency and scalability issues
Obidallah (2025) [14]	Healthcare IoT Security	Fuzzy ANP-TOPSIS	Yes	No	Yes	Yes	Not specifically designed for IoMT devices
Saad et al. (2025) [15]	Healthcare Cybersecurity	F-AHP + F-TOPSIS + FLP	Yes	No	Yes	Limited	No indeterminacy modeling
Pritika et al. (2024) [16]	IoMT Risk Assessment	Fuzzy Logic + FAHP	Yes	No	Yes	Yes	Inability to handle incomplete information
Abdalla et al. (2024) [17]	Healthcare Fuzzy Systems	Review Study	Yes	No	No	Yes	Survey-focused contribution
Khan and Ali (2024) [18]	IoHT Authentication	Graph Theory + Matrix Approach	Partial	No	Yes	Yes	Authentication-specific evaluation
Wagan et al. (2023) [19]	IoMT Anomaly Detection	FCM + Bi-LSTM	Partial	No	No	Yes	Detection rather than risk assessment
Khan et al. (2023) [20]	Authentication Assessment	AHP-TOPSIS	Limited	No	Yes	Yes	Limited cybersecurity dimensions
Proposed Study	IoMT Cybersecurity Risk Assessment	Hybrid NF AHP-SAM	Yes	Yes	Yes	Yes	Addresses ambiguity, uncertainty, inconsistency, and indeterminacy simultaneously

2.2. Cybersecurity Risks in IoMT Devices

The IoMT has been an important part of existing healthcare systems, enabling medical devices, sensors, healthcare applications and cloud platforms to communicate with each other [2,3]. IoMT technologies have enhanced patient outcomes and operational efficiency with continuous monitoring, real-time data collection, and remote healthcare services. However, the increasing inter-connectivity of medical devices has simultaneously expanded the cybersecurity attack surface, making healthcare infrastructures more vulnerable to cyber threats [4–6]. Security breaches in IoMT environments can result in unauthorized access to sensitive patient information, disruption of medical services, manipulation of device operations, and even life-threatening consequences for patients. Therefore, the understanding

and evaluation of cybersecurity risks has become a fundamental requirement for ensuring the safe and reliable deployment of IoMT technologies.

The IoMT ecosystem is exposed to cybersecurity threats from a range of sources, including device vulnerabilities, insecure communication channels, weak authentication mechanisms, software bugs, weak access controls, and evolving cyberattack methods [7–9]. Unlike conventional information systems, IoMT devices are often subjected to resource constraints and are often integrated with legacy healthcare infrastructures, which makes security management more difficult. Furthermore, the analysis of cybersecurity in healthcare environments is often subject to uncertainty, ambiguity, missing information, and conflicting expert opinions on the severity of threat and risk exposure. So, a holistic assessment framework must also consider operational criticality, threat exposure, data protection requirements, network security conditions, and organizational readiness for incident response and recovery, besides technical vulnerabilities [10–12].

To systematically assess such challenges, this study identifies seven major cybersecurity dimensions that collectively represent the security posture of IoMT environments: Identification, Vulnerability Detection, Threat Modeling, Network Security Assessment, Data Protection Assessment, Risk Scoring, and Mitigation and Response Readiness [13–17]. These dimensions are further broken down into twenty-eight sub-characteristics that address critical aspects of cybersecurity evaluation, from device criticality and software vulnerabilities to privacy compliance and incident response capability. The hierarchical structure shown in Table 3 provides a complete framework for the integrated method of NF AHP-SAM [2,4,6,10,12–16,18–20]. The integration of these dimensions and sub-characteristics into the assessment process by the framework allows for a more accurate and reliable assessment of cybersecurity risks in uncertain and indeterminate conditions, which helps informed decision-making and proactive cybersecurity management in IoMT-enabled healthcare systems.

The identified dimensions collectively provide a holistic representation of the cybersecurity risks in IoMT ecosystems. They address technical vulnerabilities, threat exposure features, network security needs, data protection issues and organizational readiness mechanisms. The incorporation of these dimensions into an integrated method of NF AHP-SAM allows a systematic assessment of cybersecurity risks in conditions of uncertain, ambiguous and incomplete information. Furthermore, the hierarchical architecture permits expert-based assessments and assists in prioritizing cybersecurity mitigation techniques to improve the resilience and trustworthiness of IoMT-enabled healthcare systems.

Table 3. Definitions of dimensions and sub-characteristics.

Dimension	Code	Sub-Characteristic	Definition
Identification (C1)	C1.1	Device Function	The primary healthcare or operational purpose performed by the IoMT device, such as monitoring, diagnosis, or treatment.
	C1.2	Connectivity Level	The degree and type of network connectivity utilized by the device (e.g., Wi-Fi, Bluetooth, cellular, cloud-connected).
	C1.3	Operational Importance	The significance of the device in supporting clinical workflows and healthcare operations.
	C1.4	Device Criticality	The potential impact on patient safety and healthcare delivery if the device becomes unavailable or compromised.
Vulnerability Detection (C2)	C2.1	Software Vulnerabilities	Security weaknesses present in the device’s operating system, applications, or embedded software.
	C2.2	Outdated Firmware	The presence of obsolete firmware versions lacking recent security patches and updates.
	C2.3	Weak Authentication	Insufficient identity verification mechanisms that may permit unauthorized access.
	C2.4	Insecure Configurations	Improper security settings or default configurations that increase exposure to cyber threats.

Table 3. Cont.

Dimension	Code	Sub-Characteristic	Definition
Threat Modeling (C3)	C3.1	Cyberattack Trends	Analysis of emerging cyber threats and attack patterns targeting healthcare and IoMT environments.
	C3.2	Exploitation Techniques	Methods and tactics used by attackers to exploit vulnerabilities in IoMT devices.
	C3.3	Device Accessibility	The ease with which attackers can physically or remotely access the device.
	C3.4	Threat Exposure Level	The likelihood of the device being targeted based on its visibility, accessibility, and attractiveness to attackers.
Network Security Assessment (C4)	C4.1	Network Segmentation	The extent to which the device is isolated from other systems to limit attack propagation.
	C4.2	Communication Encryption	The use of cryptographic protocols to protect data transmitted between devices and systems.
	C4.3	Access Control Mechanisms	Security policies and controls governing user and system access to device resources.
	C4.4	Traffic Monitoring	Continuous observation and analysis of network traffic to detect anomalies and malicious activities.
Data Protection Assessment (C5)	C5.1	Data Confidentiality	The capability to prevent unauthorized disclosure of sensitive patient and operational data.
	C5.2	Data Integrity	The assurance that data remains accurate, complete, and unaltered throughout its lifecycle.
	C5.3	Data Availability	The ability of authorized users and systems to access data whenever required.
	C5.4	Privacy Compliance	Adherence to healthcare data protection regulations, standards, and privacy requirements.
Risk Scoring (C6)	C6.1	Low Risk	A risk level indicating minimal likelihood and impact of cybersecurity incidents.
	C6.2	Medium Risk	A moderate level of cybersecurity risk requiring monitoring and mitigation efforts.
	C6.3	High Risk	A significant cybersecurity risk with substantial potential operational or patient safety consequences.
	C6.4	Critical Risk	An extremely severe risk demanding immediate intervention due to its potential impact on healthcare services.
Mitigation and Response Readiness (C7)	C7.1	Patch Management	The process of regularly applying security updates and fixes to address known vulnerabilities.
	C7.2	Incident Response Capability	The organization's preparedness to detect, contain, investigate, and recover from cybersecurity incidents.
	C7.3	Backup and Recovery Mechanisms	Procedures and technologies used to restore systems and data after failures or cyberattacks.
	C7.4	Security Awareness and Training	Programs designed to educate healthcare personnel about cybersecurity threats, policies, and best practices.

2.3. Methodology

In order to assess cybersecurity risks in IoMT environments, it is required to develop an effective methodological framework which can manage uncertainty, ambiguity, inconsistency and incomplete cybersecurity information. The evaluation of cybersecurity of IoMT ecosystems includes several interrelated aspects: device vulnerabilities, threat exposure, network security, data protection, and incident response capabilities [14,17,20–23]. The decision process is inherently complex and frequently relies on subjective expert judgment, linguistic evaluation and incomplete threat intelligence. Thus, there is a need for a strong computational framework to systematically assess and rank cybersecurity risks, given the uncertain nature of real-world healthcare environments.

Traditional MCDM methods such as AHP and ANP have been widely used for cybersecurity evaluation and risk prioritization [21–23]. These methods are useful to decompose complex problems into hierarchical structures that have criteria and sub-criteria, which help to conduct systematic evaluations and decisions. However, classical AHP assumes that the expert judgments are precise, complete and logically consistent, which is hardly true in the

context of cybersecurity risk assessment [24–26]. Experts working in IoMT environments often face uncertain threat intelligence, changing attack vectors, partial vulnerability information and inconsistent security evidence, resulting in vague and ambiguous judgments that cannot be suitably expressed by conventional crisp or fuzzy methods alone [27–29].

To overcome the above limitations, this study proposes an integrated NF AHP-SAM by combining the advantages of the neutrosophic theory and fuzzy decision-making mechanisms. In contrast to traditional fuzzy approaches that only model uncertainty and vagueness, neutrosophic theory considers the truth, indeterminacy, and falsity-membership degrees at the same time, thus providing a more comprehensive representation of ambiguous and inconsistent cybersecurity information [29,30]. The proposed framework integrates expert opinions and assesses cybersecurity risks using an NF AHP-SAM across seven major dimensions and twenty-eight sub-characteristics of IoMT security. The proposed approach uses a combination of neutrosophic and fuzzy reasoning methodology to provide a systematic, reliable and uncertainty-aware mechanism for risk evaluation, prioritization and decision support, thereby enhancing the robustness and practical applicability of cybersecurity assessments in modern IoMT-enabled healthcare systems.

The fuzzy logic theory [11] is better able to express the human understanding of crisp numbers. Therefore, it has received much attention in MCDM. Since its inception, the literature has generated a variety of approaches and ideas dealing with imprecision and uncertainty [19–21]. The Fuzzy Set theory has been rapidly generalized in the last three decades. One of the generalized forms of Fuzzy Sets is the Intuitionistic Fuzzy Sets [12] in which each element is given degrees of membership, non-membership and hesitancy. Therefore, it offers a better way to handle the vagueness and uncertainty of practical situations. However, Fuzzy Sets, although presented and generalized, cannot solve the uncertain and inconsistent information of real-life problems. For instance, one of the statements may require a professional to decide. He or she might say 0.5 is the “possibility that the statement is true”, 0.6 is the “possibility that the statement is false” and 0.2 is the “possibility that he or she is on the fence”. This example is out of the scope of FSs and IFSs, so some new concepts are needed. To overcome such situations, Smarandache [30] proposed the concept of NSs, which is an abstraction of the FSs and IFSs. The most remarkable characteristic of NS is that it is modeled by the truth-membership, indeterminacy-membership and falsity-membership functions, which belong to $[0-, 1+]$. It can describe uncertainty, imprecision, incompleteness and inconsistency.

To overcome such shortcomings, some authors proposed Fuzzy AHP, which applies Fuzzy Set theory to quantify human uncertainty by means of membership functions [27,28]. This method is more flexible but still suffers from the dualistic interpretation of the truth and falsity of the Fuzzy Set and does not offer a formal way to deal with the indeterminacy, the gray area between truth and falsehood where real-world expert opinions usually reside. This shortcoming is of utmost importance for the assessment of regulatory integration, ethical compliance and cybersecurity resilience, i.e., fields characterized by ambiguous, incomplete or contradictory expert knowledge.

The NF-AHP offers a solution to these problems by adding a third dimension, indeterminacy, to the decision continuum [29,30]. Unlike fuzzy logic, which takes into account only the degree of truth, neutrosophic logic can simultaneously and independently represent the truth (T), indeterminacy (I) and falsity (F) values for each decision element. This feature is very important in a multi-dimensional analysis of the cybersecurity risk factors evaluation where, for example, the expert panel can bring legal, technical and operational perspectives. Moreover, the NF-AHP, grounded in this triple logic, can model human reasoning by means of vagueness, inconsistency and hesitation, thus reflecting expert uncertainty in a more realistic way.

Moreover, compared to other fuzzy-based approaches such as Fuzzy Weighted Method (FWM), Fuzzy TOPSIS, or Fuzzy DEMATEL, the NF-AHP model demonstrates several methodological advantages [22–26]:

- NF-AHP allows a decomposition of complex strategic frameworks into manageable hierarchical levels, from goals to sub-characteristics.
- It retains the AHP's logical consistency check (using CI and CR) to ensure the reliability of expert judgments.
- Unlike FWSM or Fuzzy AHP, NF-AHP explicitly incorporates the “unknown” or “indeterminate” portion of expert opinion, thus reducing bias and improving decision robustness.
- NF-AHP enables both qualitative-to-quantitative transformation and deneutrosophication, translating linguistic assessments into measurable, comparable results.
- Through its ability to handle contradictory expert inputs, NF-AHP minimizes sensitivity to extreme judgments and stabilizes final ranking outcomes.

A symmetrical hybrid neutrosophic fuzzy-based framework is a robust and efficient analytical tool to assess complex cybersecurity parameters under uncertain circumstances for the purpose of cybersecurity risk assessment in IoMT environments. The developed framework offers a holistic evaluation of various aspects of cybersecurity such as device identification, Vulnerability Detection, Threat Modeling, network security, data security, severity of risk, and mitigation preparedness. Moreover, it successfully integrates the diverse perspectives of cybersecurity experts, healthcare workers, network administrators, and IoMT experts, thereby providing a comprehensive and realistic assessment process.

The combination of neutrosophic set theory and fuzzy decision-making techniques significantly enhances the capacity of the assessment framework to handle uncertainty, ambiguity, inconsistency, and incomplete cybersecurity information. The proposed NF AHP-SAM captures the truth, indeterminacy and falsity-membership values of expert opinions, unlike traditional risk assessment methods that assume precise and consistent judgments. This capability is particularly critical in IoMT cybersecurity settings where threat intelligence is often fragmentary, attack patterns are continually changing, and experts may have divergent levels of confidence in the severity and probability of cyber threats. The framework thus offers more reliable, realistic and robust cybersecurity risk assessments.

The integrated method of NF AHP-SAM is a sophisticated symmetrical methodical approach for evaluation of cybersecurity risks in IoMT devices and healthcare eco-systems. The proposed framework combines the flexibility of fuzzy reasoning and the enhanced uncertainty modeling capacity of neutrosophic theory, and hence it offers both conceptual comprehensiveness and computational rigor. The resulting risk prioritization outcomes allow healthcare organizations, security analysts, and policy-makers to identify critical vulnerabilities, allocate cybersecurity resources effectively, and implement proactive mitigation strategies to enhance the resilience, reliability, and trustworthiness of IoMT-enabled healthcare systems.

2.3.1. Relevant Definitions

In this study, a hybrid neutrosophic fuzzy-based framework is used to evaluate and rank cybersecurity risks in IoMT environments. Neutrosophic theory offers a powerful instrument for dealing with uncertainty, ambiguity, indeterminacy and incomplete information, which are always present in cybersecurity evaluations and expert assessments. The suggested framework integrates neutrosophic reasoning and fuzzy decision-making for a more reliable and realistic assessment of cybersecurity risk factors that contribute to effective prioritization and informed decision-making in IoMT-enabled healthcare systems.

A single-valued neutrosophic fuzzy number (SVNFN) is represented as $T = ((l, m, u)T_a, I_a, F_a)$, where l , m , and u denote the lower, modal, and upper values of the triangular fuzzy number, respectively, while T_a , I_a , and F_a denote the degrees of truth, indeterminacy, and falsity, respectively, and are real numbers within the interval $[0, 1]$. The basic operations among two single-valued neutrosophic fuzzy numbers $T_1 = (T_{a1}, I_{a1}, F_{a1})$ and $T_2 = (T_{a2}, I_{a2}, F_{a2})$ are expressed as follows:

Addition of neutrosophic fuzzy numbers is given by

$$T_1 + T_2 = (T_{a1} + T_{a2} - T_{a1}T_{a2}, I_{a1}I_{a2}, F_{a1}F_{a2}) \quad (1)$$

Multiplication is defined as

$$T_1 * T_2 = (T_{a1}T_{a2}, I_{a1} + I_{a2} - I_{a1}I_{a2}, F_{a1} + F_{a2} - F_{a1}F_{a2}) \quad (2)$$

Division is represented by

$$\frac{T_2}{T_1} = \left(\frac{T_{a2}}{T_{a1}}, \frac{I_{a2} - I_{a1}}{1 - I_{a1}}, \frac{F_{a2} - F_{a1}}{1 - F_{a1}} \right) \quad (3)$$

For a scalar $A > 0$, the division and multiplication with a neutrosophic number T_1 are defined as

$$\frac{T_1}{A} = \left(1 - (1 - T_{a1})^{1/A}, I_{a1}^{1/A}, F_{a1}^{1/A} \right) \quad (4)$$

$$A * T_1 = \left(1 - (1 - T_{a1})^A, I_{a1}^A, F_{a1}^A \right) \quad (5)$$

To convert neutrosophic values into a crisp score, the deneutrosophication process uses a score function $S(T_1)$ defined as

$$S(T_1) = \frac{(3 + T_{a1} - 2I_{a1} - F_{a1})}{4} \quad (6)$$

This score function translates fuzzy judgments into deterministic numerical values, facilitating pairwise comparison and weight derivation.

2.3.2. NF-AHP Approach

One of the most popular MCDM methods for breaking down complex decision problems into hierarchical structures of criteria and sub-criteria is the AHP method proposed by Saaty [23–25]. However, the traditional AHP assumes that the experts' judgments are accurate and consistent. This is not always the case in cybersecurity risk assessment contexts due to uncertainty, ambiguity, incomplete information, and dynamic threat environments. To overcome the above limitations, the present study proposes a hybrid neutrosophic fuzzy-based framework that integrates neutrosophic logic with hierarchical decision-making principles, which allows the representation of expert evaluations through truth, indeterminacy and falsity-membership values.

The relative importance of seven major cybersecurity dimensions and their twenty-eight associated sub-characteristics for assessing cybersecurity risks in IoMT environments is presented in Table 3, and it is evaluated using the proposed framework. Expert opinions were gathered from cybersecurity professionals, healthcare technology specialists, network security practitioners, and experts in the IoMT domain. The framework systematically aggregates expert judgements using the NF AHP-SAM to derive the importance ratings and prioritizes cybersecurity risk factors (Figure 1).

Step 1: Hierarchy Design: The first step is to define the overall objective, and the problem is then structured into a hierarchical framework of three levels (Table 3) [26–28].

The highest level is the objective of the assessment. Level 1 consists of seven cybersecurity dimensions, namely Identification (C1), Vulnerability Detection (C2), Threat Modeling (C3), Network Security Assessment (C4), Data Protection Assessment (C5), Risk Scoring (C6), and Mitigation and Response Readiness (C7). Twenty-eight sub-characteristics are included in Level 2 for these dimensions. This hierarchical decomposition allows for a thorough and systematic evaluation of cybersecurity risks by explicitly modeling the contribution of each criterion and sub-criterion to the overall security assessment of IoMT environments.

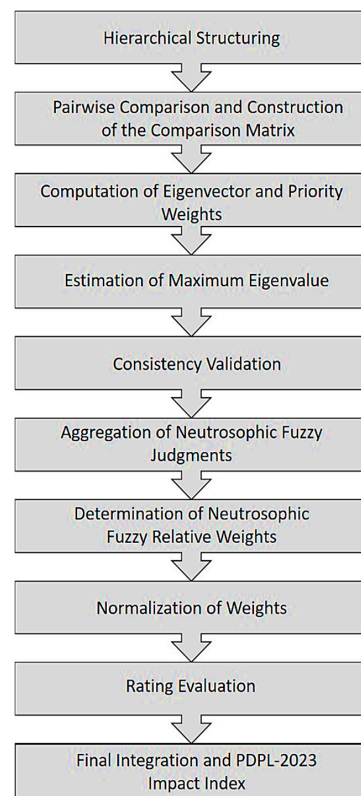


Figure 1. Workflow of the methodology.

Step 2: Pairwise Comparison and the Formation of the Comparison Matrix: Expert judgments are gathered using a 1–9 neutrosophic fuzzy scale (see Table 4) [24]. Where (l, m, u) denotes the triangular fuzzy number (lower, middle, and upper values), T represents the truth-membership degree, I indicates the indeterminacy-membership degree, and F denotes the falsity-membership degree. Each comparison between criteria i and j yields a neutrosophic fuzzy number a_{ij} , forming a pairwise comparison matrix $A = \{a_{ij}\}$.

Table 4. Neutrosophic Fuzzy Set scale.

Saaty Scale	Linguistic Term	Neutrosophic TFN $((l, m, u); T, I, F)$
1	Equally Significant	$((1, 1, 1); 0.50, 0.50, 0.50)$
3	Slightly Significant	$((2, 3, 4); 0.30, 0.75, 0.70)$
5	Strongly Significant	$((4, 5, 6); 0.80, 0.15, 0.20)$
7	Very Strongly Significant	$((6, 7, 8); 0.90, 0.10, 0.10)$
9	Absolutely Significant	$((9, 9, 0); 1.00, 0.00, 0.00)$
2	Periodic values between two close scales	$((1, 2, 3); 0.40, 0.60, 0.65)$
4		$((3, 4, 5); 0.35, 0.60, 0.40)$
6		$((5, 6, 7); 0.70, 0.25, 0.30)$
8		$((7, 8, 9); 0.85, 0.10, 0.15)$

The fundamental condition holds:

$$a_{ij} = 1/a_{ji} \quad (7)$$

Step 3: Computation of Eigenvector and Priority Weights: The principal right eigenvector W of the pairwise comparison matrix A is derived as

$$e^T = (1, 1, \dots, 1) \quad (8)$$

$$W = \lim_{k \rightarrow \infty} \frac{A^k \cdot e}{e^T \cdot A^k \cdot e} \quad (9)$$

This eigenvector represents the relative weights (priorities) of criteria under evaluation.

Step 4: Estimation of Maximum Eigenvalue: To ensure consistency of expert judgments, the maximum eigenvalue γ_{max} of the matrix is calculated as

$$Aw = \gamma_{max}, \gamma_{max} \geq n \quad (10)$$

$$\gamma_{max} = \frac{\sum a_j w_j - n}{w_1} \quad (11)$$

where n denotes the matrix dimension, and w_j is the normalized weight of criterion j .

Step 5: Consistency Validation: The Consistency Index (CI) and Consistency Ratio (CR) are used to verify logical consistency:

$$CI = \frac{\gamma_{max} - n}{n - 1} \quad (12)$$

$$CR = \frac{CI}{RI} \quad (13)$$

If $CR < 0.10$, the matrix is deemed consistent. RI values depend on matrix size (refer to Table 5). According to Saaty's AHP consistency criteria [24], a comparison matrix is considered acceptably consistent when the CR is less than 0.10. This threshold indicates that the degree of inconsistency in the pairwise judgments is sufficiently low, ensuring the reliability of the derived priority weights for decision-making.

Table 5. Random Index Scale.

Dimension	RI
1	0
2	0
3	0.5799
4	0.8921
5	1.1159
6	1.2358
7	1.3322
8	1.3952
9	1.4537
10	1.4882

Step 6: Aggregation of Neutrosophic Fuzzy Judgments: Individual expert opinions are aggregated using the neutrosophic Fuzzy Weighted arithmetic mean:

$$T_{group} = 1/m \sum_{k=1}^m Tk \quad (14)$$

where Tk is the neutrosophic fuzzy judgment of the k^{th} expert and m is the number of experts. This step captures diverse perspectives while preserving uncertainty and indeterminacy.

Step 7: Determination of Neutrosophic Fuzzy Relative Weights: The aggregated pairwise matrices are processed through the eigenvector method under neutrosophic operations (Equations (1)–(5)). The resulting fuzzy weights for each criterion represent the integrated significance of dimensions.

Step 8: Normalization of Weights: All neutrosophic fuzzy weights are normalized to ensure that the total sum equals one:

$$W_{norm,i} = W_i / \sum W_i \quad (15)$$

These normalized weights express the proportionate influence of each phase or sub-characteristic within the framework.

Step 9: Determination of Neutrosophic Fuzzy Rating: The SAM is used to aggregate multiple expert ratings expressed in neutrosophic triangular fuzzy form [28].

Let K experts evaluate alternative A_i under criterion C_j using a single-valued neutrosophic triangular fuzzy number (SVNTFN). The rating given by the K th expert is expressed as Equation (16) with the help of Table 6 [29].

$$\tilde{x}_{ij}^{(k)} = \left(\left(l_{ij}^{(k)}, m_{ij}^{(k)}, u_{ij}^{(k)} \right), T_{ij}^{(k)}, I_{ij}^{(k)}, F_{ij}^{(k)} \right) \quad (16)$$

where A_i denotes the i th alternative and C_j denotes the j th evaluation criterion.

Table 6. Linguistic rating scale and corresponding single-valued neutrosophic triangular fuzzy numbers.

Saaty Scale	Linguistic Rating	l, m, u	T	I	F
1	Very Poor (VP)	(1, 1, 2)	0.30	0.60	0.70
2	Poor–Very Poor	(1, 2, 3)	0.40	0.50	0.60
3	Poor (P)	(2, 3, 4)	0.50	0.45	0.50
4	Slightly Poor	(3, 4, 5)	0.60	0.40	0.40
5	Fair (F)	(4, 5, 6)	0.70	0.35	0.30
6	Fair–Good	(5, 6, 7)	0.80	0.30	0.25
7	Good (G)	(6, 7, 8)	0.85	0.25	0.20
8	Very Good	(7, 8, 9)	0.90	0.20	0.15
9	Excellent (E)	(8, 9, 9)	0.95	0.15	0.10

If K experts provide evaluations, the aggregated rating using the SAM [28] operator is calculated as

$$\tilde{x}_{ij} = \frac{1}{K} \sum_{k=1}^K \tilde{x}_{ij}^{(k)} \quad (17)$$

The aggregated rating is computed component-wise as

$$\tilde{x}_{ij} = \left(\left(\frac{1}{K} \sum_{k=1}^K l_{ij}^{(k)}, \frac{1}{K} \sum_{k=1}^K m_{ij}^{(k)}, \frac{1}{K} \sum_{k=1}^K u_{ij}^{(k)} \right); \frac{1}{K} \sum_{k=1}^K T_{ij}^{(k)}, \frac{1}{K} \sum_{k=1}^K I_{ij}^{(k)}, \frac{1}{K} \sum_{k=1}^K F_{ij}^{(k)} \right) \quad (18)$$

Step 10: Final Integration and Cybersecurity Risks Index: The final step involves synthesizing normalized and deneutrosophicated weights to compute the Cybersecurity Risk Index (CRI) [25–28]:

$$CRI = \sum_{i=1}^n (W_{norm,i} * S_i) \quad (19)$$

This index quantitatively expresses the degree of cybersecurity risks alignment and effectiveness, allowing comparison across entities or operational domains.

3. Numerical Analysis and Results

This paper used a symmetrical integrated approach of NF AHP-SAM for prioritizing and assessing cybersecurity risks in IoMT environments. The framework combines neutrosophic theory and fuzzy decision-making to tackle the uncertainty, ambiguity, inconsistency,

and incomplete information that typically appear in cybersecurity assessments. The proposed methodology differs from traditional risk assessment approaches by simultaneously considering the truth, indeterminacy, and falsity of expert judgments, which results in a more realistic representation of cybersecurity risk perceptions within healthcare ecosystems.

The computational analysis began with the collection of the expert assessments in the form of SVNFNs. Each assessment was expressed by truth, indeterminacy and falsity-membership values, allowing experts to express different levels of confidence in their judgments. Then, the neutrosophic aggregation and the arithmetic operations were used to aggregate the individual opinions and construct pairwise comparison matrices for the seven cybersecurity dimensions and twenty-eight sub-characteristics, as identified in Table 4. This process converted qualitative cybersecurity assessments into structured quantitative data that can be analyzed computationally.

A multidisciplinary panel of 137 experts conducted an evaluation process. The panel featured cybersecurity professionals, healthcare technology specialists, network security analysts, digital forensics experts, and IoMT practitioners with 10–15 years of experience in healthcare cybersecurity and critical infrastructure protection, representing both academia and industry. Experts were selected according to a set of predefined eligibility criteria, such as professional experience, cybersecurity expertise, involvement in healthcare technology projects, and knowledge of IoMT security challenges, using a purposive sampling method. To protect confidentiality and adhere to ethical standards, all personal identifiers have been removed, and only generalized demographic and professional information is reported. To enhance transparency, reproducibility, and methodological clarity, Appendix A presents a representative sample of the questionnaire used for expert elicitation, while the complete dataset supporting the analysis has been provided as a Supplementary File accompanying this manuscript.

The experts employed pairwise comparisons to assess the relative importance of the seven cybersecurity dimensions and their associated sub-characteristics. The linguistic expressions “equally important”, “moderately important”, “strongly important” and “extremely important” were converted into the corresponding neutrosophic fuzzy numbers according to the predefined linguistic scale. The pairwise comparison relationships were maintained reciprocally to preserve the logical consistency of the evaluation process.

Then, priority weights and importance scores were computed through a hybrid neutrosophic fuzzy-based framework. The reliability of expert judgments was verified through consistency analysis. For all the matrices of comparison, the CI and CR have been calculated. The values obtained for CR stayed under the acceptable threshold of 0.10, which is proof of consistency and reliability of the expert evaluations.

After the consistency check, the respective neutrosophic ratings were aggregated using NF AHP-SAM. The aggregation process preserves the intrinsic uncertainty and indeterminacy of expert opinions, but also yields collective evaluations for each of the cybersecurity dimensions and sub-characteristics. The aggregated neutrosophic values were then normalized and turned into crisp scores through a deneutrosophication process, which allowed for the quantitative ranking and prioritization of the cybersecurity risks.

The final cybersecurity risk scores were calculated by combining the normalized weights and the aggregated ratings for all the dimensions and sub-characteristics. The generated *CRI* is a metric to measure the overall cybersecurity posture of IoMT environments. The higher the *CRI* value, the higher the exposure to cyber risks and the more severe the risk; the lower the *CRI* value, the stronger the security controls and the better the resilience to cyber threats.

The final cybersecurity risk scores were obtained by combining the normalized criterion weights with the aggregated neutrosophic ratings of all dimensions and their cor-

responding sub-characteristics. The resulting *CRI* provides a quantitative measure of the overall cybersecurity posture of IoMT environments. In the proposed framework, a higher *CRI* indicates greater exposure to cybersecurity threats and a higher overall risk level, whereas a lower *CRI* reflects stronger security controls, enhanced resilience, and improved preparedness against cyber threats. The proposed framework produced a *CRI* value of 0.8504, indicating a relatively high cybersecurity risk level and emphasizing the need for prioritized mitigation strategies to strengthen the security posture of IoMT systems.

At the dimension level, Data Protection Assessment (C5) achieved the highest normalized weight, followed by Identification (C1), Network Security Assessment (C4), Vulnerability Detection (C2), Risk Scoring (C6), Threat Modeling (C3), and Mitigation and Response Readiness (C7). These results indicate that protecting sensitive healthcare data, accurately identifying critical medical devices, and securing communication networks are the most influential factors affecting the cybersecurity posture of IoMT environments. Although Mitigation and Response Readiness (C7) received the lowest normalized weight, it remains an essential component of the overall cybersecurity strategy, highlighting opportunities to further strengthen organizational preparedness, incident response capabilities, and cybersecurity awareness.

At the sub-characteristic level, Data Confidentiality (C5.1) obtained the highest global weight, followed by Device Function (C1.1), Data Integrity (C5.2), Network Segmentation (C4.1), and Data Availability (C5.3). These findings emphasize that protecting sensitive healthcare information while ensuring its confidentiality, integrity, and availability constitutes the primary cybersecurity priority in IoMT environments. Furthermore, the high rankings of Device Function and Network Segmentation demonstrate the importance of correctly identifying critical medical devices and implementing secure network architectures to reduce the attack surface and improve cyber resilience. Collectively, the obtained rankings provide a systematic basis for prioritizing cybersecurity investments and mitigation strategies, enabling healthcare organizations to allocate resources more effectively toward the most critical security requirements.

The combined NF AHP-SAM approach effectively generated a detailed prioritization of cybersecurity risks in IoMT settings. To handle the uncertainty and indeterminacy of expert judgements efficiently, neutrosophic reasoning was incorporated. The NF AHP-SAM aggregation mechanism provided reliable and consistent evaluation results. The resulting rankings help healthcare organizations, cybersecurity practitioners, and policymakers to identify critical vulnerabilities, allocate security resources efficiently, and implement proactive risk mitigation strategies.

The SAM is adopted in this study to aggregate the neutrosophic fuzzy evaluations obtained from multiple domain experts. The selection of SAM is motivated by both theoretical considerations and the characteristics of the IoMT cybersecurity evaluation scenario. Specifically, all participating experts were selected using predefined eligibility criteria and possessed comparable expertise in cybersecurity risk assessment, healthcare systems, and IoMT security. Since no objective evidence, historical performance records, or quantitative measures were available to distinguish the reliability of one expert from another, assigning unequal expert weights would have introduced unnecessary subjectivity into the aggregation process. Therefore, treating all expert opinions equally through SAM provides an objective, transparent, and unbiased mechanism for obtaining the collective assessment.

Furthermore, the proposed framework explicitly models uncertainty, indeterminacy, and inconsistency using NFS. Consequently, the primary role of the aggregation operator is not to model uncertainty itself, but rather to combine individual neutrosophic expert evaluations into a unified decision while preserving transparency, interpretability, and computational efficiency.

Compared with more sophisticated aggregation operators, such as the weighted average, Ordered Weighted Averaging (OWA), and geometric mean, SAM does not require additional parameter estimation, optimization, or expert-weight assignment. This makes it particularly suitable for decision-making scenarios in which all experts are intentionally selected to have comparable qualifications and experience. Moreover, the simplicity of SAM enhances the reproducibility and practical applicability of the proposed framework for cybersecurity risk assessment in IoMT environments.

Previous research has demonstrated the effectiveness of integrating Fuzzy AHP with SAM for decision-making applications [28]. Building upon this foundation, the present study extends the methodology by integrating NFSs with AHP and SAM, enabling the simultaneous representation of truth, indeterminacy, and falsity in expert judgments while maintaining a simple, transparent, and computationally efficient aggregation process. To the best of the author's knowledge, this hybrid NFS-AHP-SAM framework has not previously been applied to cybersecurity risk assessment in IoMT environments.

Future research will investigate alternative aggregation operators, including the weighted average, OWA, geometric mean, and other advanced neutrosophic aggregation techniques, to compare their performance with the proposed SAM-based framework and evaluate their impact on cybersecurity risk assessment outcomes.

The computation process began with the collection of the 137 expert judgments to construct the collective neutrosophic comparison matrix (Table 7). Then, the priority weights and normalized scores of the seven cybersecurity dimensions were calculated (Table 8). Table 9 and Figure 2 show the deneutrosophicated crisp values, cybersecurity risk ratings and final rankings of the dimensions and sub-characteristics, respectively.

Table 7. Aggregated neutrosophic fuzzy comparison matrix at Level 1.

Dimension	C1	C2	C3	C4	C5	C6	C7
C1	(1.00, 1.00, 1.00)	(0.62, 0.18, 0.20)	(0.68, 0.16, 0.22)	(0.75, 0.14, 0.18)	(0.60, 0.20, 0.25)	(0.80, 0.10, 0.15)	(0.72, 0.15, 0.20)
C2	(0.38, 0.82, 0.80)	(1.00, 1.00, 1.00)	(0.70, 0.18, 0.22)	(0.66, 0.20, 0.24)	(0.58, 0.22, 0.26)	(0.62, 0.18, 0.22)	(0.75, 0.14, 0.18)
C3	(0.32, 0.84, 0.78)	(0.30, 0.82, 0.78)	(1.00, 1.00, 1.00)	(0.64, 0.20, 0.25)	(0.55, 0.25, 0.28)	(0.68, 0.16, 0.22)	(0.72, 0.15, 0.20)
C4	(0.25, 0.86, 0.82)	(0.34, 0.80, 0.76)	(0.36, 0.78, 0.74)	(1.00, 1.00, 1.00)	(0.65, 0.20, 0.24)	(0.70, 0.18, 0.22)	(0.75, 0.14, 0.18)
C5	(0.40, 0.80, 0.75)	(0.42, 0.78, 0.72)	(0.45, 0.74, 0.68)	(0.35, 0.82, 0.78)	(1.00, 1.00, 1.00)	(0.80, 0.10, 0.15)	(0.85, 0.08, 0.12)
C6	(0.20, 0.90, 0.85)	(0.38, 0.82, 0.78)	(0.32, 0.84, 0.78)	(0.30, 0.86, 0.80)	(0.20, 0.90, 0.85)	(1.00, 1.00, 1.00)	(0.68, 0.16, 0.22)
C7	(0.28, 0.84, 0.78)	(0.25, 0.86, 0.82)	(0.28, 0.84, 0.78)	(0.25, 0.86, 0.82)	(0.15, 0.92, 0.88)	(0.32, 0.84, 0.78)	(1.00, 1.00, 1.00)

Table 8. Normalized neutrosophic weights at Level 1.

Dimension	Neutrosophic Weight	Normalized Weight	Ranking
Identification (C1)	(0.84, 0.11, 0.12)	0.164	2
Vulnerability Detection (C2)	(0.80, 0.13, 0.15)	0.155	4
Threat Modeling (C3)	(0.76, 0.14, 0.17)	0.149	6
Network Security Assessment (C4)	(0.82, 0.12, 0.14)	0.160	3
Data Protection Assessment (C5)	(0.88, 0.09, 0.10)	0.172	1
Risk Scoring (C6)	(0.78, 0.14, 0.16)	0.152	5
Mitigation and Response Readiness (C7)	(0.74, 0.15, 0.18)	0.147	7

Table 9. Rating scores at Level 1.

Dimension	Symbol	L	M	U	Score	Rating
Identification (C1)	C1	0.82	0.84	0.86	0.84	2
Vulnerability Detection (C2)	C2	0.78	0.80	0.82	0.80	4
Threat Modeling (C3)	C3	0.74	0.76	0.78	0.76	6
Network Security Assessment (C4)	C4	0.80	0.82	0.84	0.82	3
Data Protection Assessment (C5)	C5	0.86	0.88	0.90	0.88	1
Risk Scoring (C6)	C6	0.76	0.78	0.80	0.78	5
Mitigation and Response Readiness (C7)	C7	0.72	0.74	0.76	0.74	7

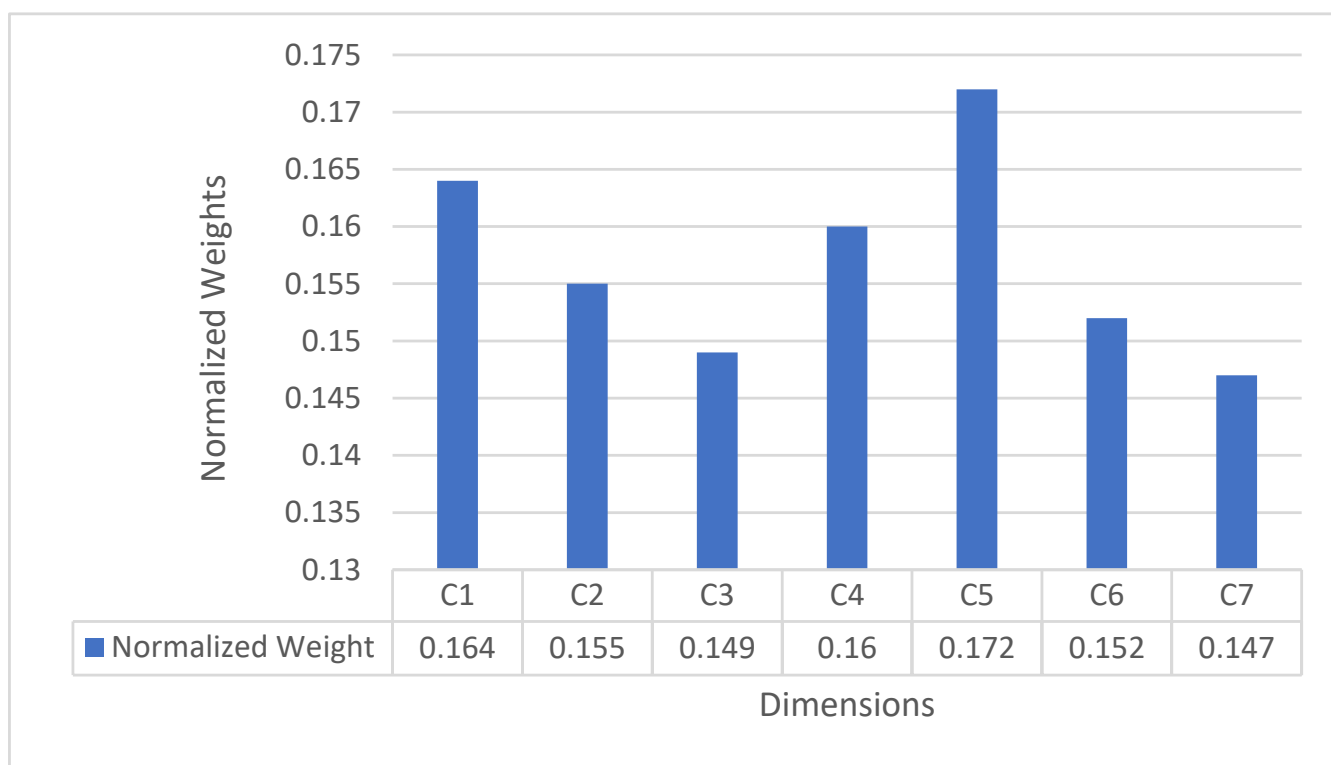


Figure 2. Graphical representation of initial level ranking.

Results showed that Data Protection Assessment (C5) is the most important cybersecurity dimension, ranked first, highlighting the importance of software vulnerabilities, old firmware, weak authentication mechanisms, and insecure configurations in the overall security posture of IoMT environments. Next up were Identification (C1) and Network Security Assessment (C4). It is important to note that cyber threats are constantly changing, the way they are exploited, how exposed the devices are, how secure communication is, and the access control mechanisms. Results show that technical vulnerabilities and threat exposure continue to be the main drivers of cybersecurity risks in healthcare IoMT ecosystems.

In contrast, Threat Modeling (C3) and Mitigation and Response Readiness (C7) were ranked relatively low. While these dimensions are still important for protecting confidentiality, integrity, availability, regulatory compliance and response readiness, the findings suggest that organizations are more inclined to detect and prevent cyber threats than to recover from incidents and build long-term resilience strategies. However, the relatively lower rankings should not be interpreted as lower importance but as indicators of areas that need further investment and continuous improvement to enhance the overall cybersecurity maturity.

Figure 3 shows the graphical representation of the importance ratings obtained for seven cybersecurity dimensions. The analysis was also conducted at the sub-characteristic level (C1.1–C7.4) to gain an understanding of the role of each cybersecurity factor in contributing to the overall CRI. An integrated method of NF AHP-SAM was used for systematic analysis of expert evaluations to determine local and global importance weights for all twenty-eight sub-characteristics. The aggregated neutrosophic fuzzy values were normalized and deneutrosophicated to obtain crisp scores, which enabled accurate prioritization of cybersecurity risk factors. Tables 10 and 11 and Figure 4 show the resulting rankings, giving a comprehensive multidimensional evaluation of IoMT cybersecurity risks and identifying the most dominant factors influencing the security, resilience and trustworthiness of IoMT-empowered healthcare systems.

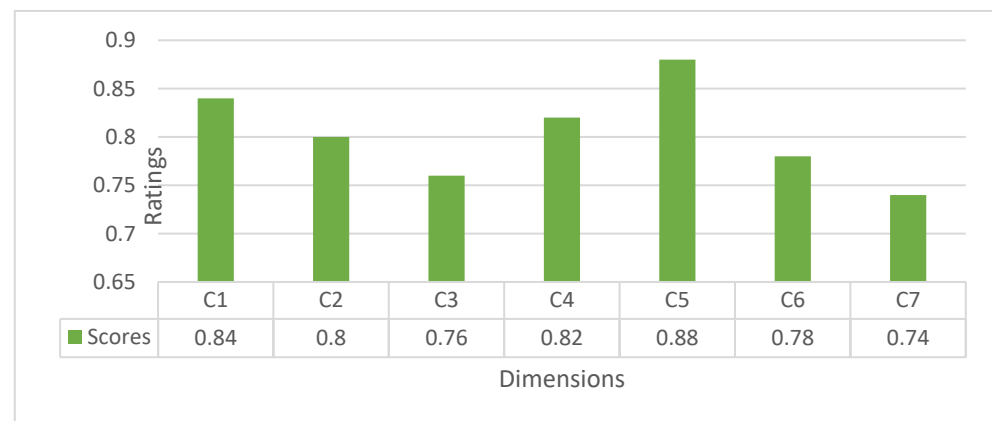


Figure 3. Graphical representation of initial level rating score.

Table 10. Normalized local and global weights at the final level characteristics.

Dimension	Symbol	Sub-Characteristic	Neutrosophic Weight	Normalized Local Weight	Global Weight	Global Ranking
Identification (C1)	C1.1	Device Function	(0.86, 0.10, 0.12)	0.286	0.0469	2
	C1.2	Connectivity Level	(0.82, 0.12, 0.14)	0.252	0.0413	6
	C1.3	Operational Importance	(0.78, 0.14, 0.16)	0.236	0.0387	11
	C1.4	Device Criticality	(0.80, 0.13, 0.15)	0.226	0.0371	20
Vulnerability Detection (C2)	C2.1	Software Vulnerabilities	(0.84, 0.11, 0.13)	0.264	0.0409	7
	C2.2	Outdated Firmware	(0.80, 0.12, 0.15)	0.247	0.0383	14
	C2.3	Weak Authentication	(0.78, 0.13, 0.16)	0.243	0.0377	17
	C2.4	Insecure Configurations	(0.76, 0.14, 0.17)	0.246	0.0381	16
Threat Modeling (C3)	C3.1	Cyberattack Trends	(0.80, 0.13, 0.15)	0.261	0.0386	13
	C3.2	Exploitation Techniques	(0.76, 0.14, 0.17)	0.247	0.0366	26
	C3.3	Device Accessibility	(0.75, 0.15, 0.18)	0.244	0.0361	28
	C3.4	Threat Exposure Level	(0.74, 0.15, 0.18)	0.248	0.0367	25
Network Security Assessment (C4)	C4.1	Network Segmentation	(0.83, 0.11, 0.13)	0.270	0.0432	4
	C4.2	Communication Encryption	(0.80, 0.13, 0.15)	0.252	0.0403	8
	C4.3	Access Control Mechanisms	(0.78, 0.14, 0.16)	0.245	0.0392	9
	C4.4	Traffic Monitoring	(0.76, 0.14, 0.17)	0.233	0.0373	19
Data Protection Assessment (C5)	C5.1	Data Confidentiality	(0.88, 0.09, 0.10)	0.276	0.0475	1
	C5.2	Data Integrity	(0.86, 0.10, 0.12)	0.263	0.0452	3
	C5.3	Data Availability	(0.82, 0.11, 0.13)	0.246	0.0423	5
	C5.4	Privacy Compliance	(0.78, 0.13, 0.15)	0.215	0.0370	22
Risk Scoring (C6)	C6.1	Low Risk	(0.80, 0.13, 0.15)	0.258	0.0392	10
	C6.2	Medium Risk	(0.78, 0.14, 0.16)	0.251	0.0382	15
	C6.3	High Risk	(0.77, 0.15, 0.17)	0.247	0.0375	18
	C6.4	Critical Risk	(0.75, 0.15, 0.18)	0.244	0.0371	21
Mitigation and Response Readiness (C7)	C7.1	Patch Management	(0.78, 0.14, 0.16)	0.260	0.0387	12
	C7.2	Incident Response Capability	(0.76, 0.14, 0.17)	0.248	0.0370	23
	C7.3	Backup and Recovery Mechanisms	(0.74, 0.15, 0.18)	0.247	0.0368	24
	C7.4	Security Awareness and Training	(0.74, 0.15, 0.18)	0.245	0.0365	27

Table 11. Global rating scores at the final level characteristics.

Dimension	Symbol	Sub-Characteristic	Local Score	Parent Score	Global Score	Global Rating
Identification (C1)	C1.1	Device Function	0.91	0.90	0.819	3
	C1.2	Connectivity Level	0.89	0.90	0.801	5
	C1.3	Operational Importance	0.87	0.90	0.783	10
	C1.4	Device Criticality	0.88	0.90	0.792	8
Vulnerability Detection (C2)	C2.1	Software Vulnerabilities	0.90	0.88	0.792	9
	C2.2	Outdated Firmware	0.88	0.88	0.774	12
	C2.3	Weak Authentication	0.87	0.88	0.766	14
	C2.4	Insecure Configurations	0.86	0.88	0.757	17
Threat Modeling (C3)	C3.1	Cyberattack Trends	0.88	0.86	0.757	18
	C3.2	Exploitation Techniques	0.86	0.86	0.740	21
	C3.3	Device Accessibility	0.85	0.86	0.731	24
	C3.4	Threat Exposure Level	0.85	0.86	0.731	25
Network Security Assessment (C4)	C4.1	Network Segmentation	0.90	0.89	0.801	6
	C4.2	Communication Encryption	0.88	0.89	0.783	11
	C4.3	Access Control Mechanisms	0.87	0.89	0.774	13
	C4.4	Traffic Monitoring	0.86	0.89	0.765	16

Table 11. Cont.

Dimension	Symbol	Sub-Characteristic	Local Score	Parent Score	Global Score	Global Rating
Data Protection Assessment (C5)	C5.1	Data Confidentiality	0.92	0.92	0.846	1
	C5.2	Data Integrity	0.91	0.92	0.837	2
	C5.3	Data Availability	0.89	0.92	0.819	4
	C5.4	Privacy Compliance	0.87	0.92	0.800	7
Risk Scoring (C6)	C6.1	Low Risk	0.88	0.87	0.766	15
	C6.2	Medium Risk	0.87	0.87	0.757	19
	C6.3	High Risk	0.86	0.87	0.748	20
	C6.4	Critical Risk	0.85	0.87	0.740	22
Mitigation and Response Readiness (C7)	C7.1	Patch Management	0.87	0.85	0.740	23
	C7.2	Incident Response Capability	0.86	0.85	0.731	26
	C7.3	Backup and Recovery Mechanisms	0.85	0.85	0.723	27
	C7.4	Security Awareness and Training	0.85	0.85	0.723	28

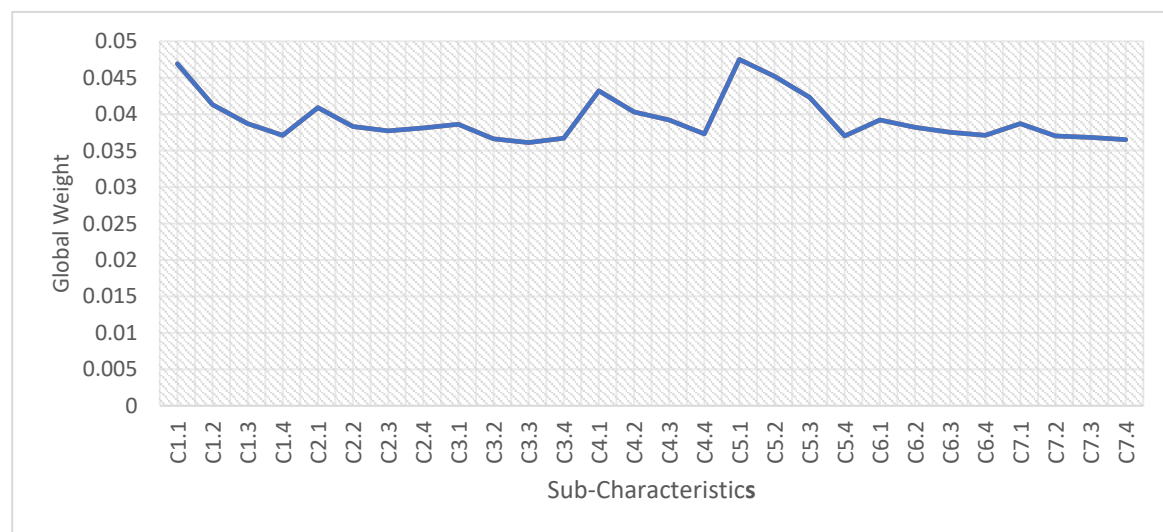


Figure 4. Graphical representation of global ranking at the final level characteristics.

Table 10 presents the normalized local weights and global weights of the twenty-eight cybersecurity sub-characteristics obtained using a hybrid neutrosophic fuzzy-based framework. Initially, the aggregated neutrosophic fuzzy evaluations expressed through truth, indeterminacy, and falsity memberships are transformed into crisp values. These values are subsequently normalized within each cybersecurity dimension to derive the local weights, ensuring that the sum of weights within each dimension equals one. The global weight of each sub-characteristic is then computed by multiplying its normalized local weight by the corresponding weight of its parent cybersecurity dimension. The resulting global weights provide a quantitative measure of the relative importance of each cybersecurity factor within the overall IoMT cybersecurity assessment framework and facilitate their prioritization.

Table 11 shows the global cybersecurity risk ratings for each sub-characteristic and Figure 5 shows the graphical representation of the same. The overall score of a sub-characteristic is obtained by multiplying the importance weight of the parent dimension to which the sub-characteristic belongs by the local performance rating of the sub-characteristic. Therefore, the global score is the sum of the contribution of the single sub-characteristic and the influence of the global cybersecurity dimension to which it belongs. These scores give a holistic view of the cybersecurity posture of IoMT environments by identifying the factors that contribute most to the overall cybersecurity risk. The global scores provide the rankings, which offer useful insights into the critical areas that need better security controls, monitoring and mitigation efforts.

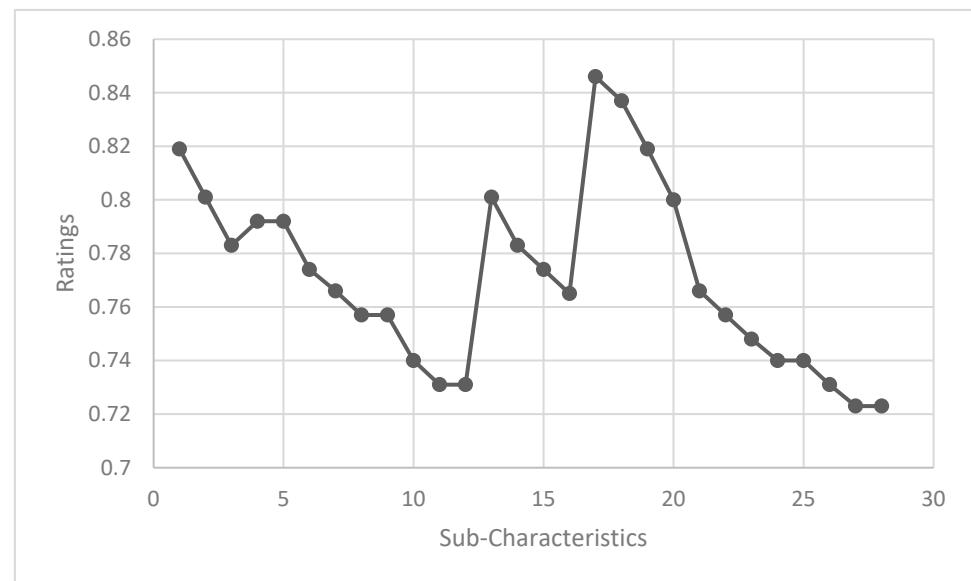


Figure 5. Graphical representation of global ratings.

The seven cybersecurity dimensions (C1–C7) with four sub-characteristics each contribute towards the final *CRI* through the normalized local and global weights generated using a hybrid neutrosophic fuzzy-based framework. This structured assessment provides a holistic picture of the relative importance and impact of individual cybersecurity factors across the IoMT ecosystem. The final *CRI* is calculated by multiplying the global weights from Table 10 with the corresponding global ratings in Table 11. For example, if the global weight and global rating of sub-characteristic C1.1 are represented by $0.0469 \times 0.819 = 0.0384$. Similarly, the overall *CRI* is obtained by summing such contributions across all sub-characteristics:

$$\begin{aligned}
 CRI = & (0.0469 \times 0.819) + (0.0413 \times 0.801) + (0.0387 \times 0.783) + (0.0371 \times 0.792) + (0.0409 \times 0.792) + (0.0383 \times 0.774) \\
 & + (0.0377 \times 0.766) + (0.0381 \times 0.757) + (0.0386 \times 0.757) + (0.0366 \times 0.740) + (0.0361 \times 0.731) + (0.0367 \times 0.731) \\
 & + (0.0432 \times 0.801) + (0.0403 \times 0.783) + (0.0392 \times 0.774) + (0.0373 \times 0.765) + (0.0475 \times 0.846) + (0.0452 \times 0.837) \\
 & + (0.0423 \times 0.819) + (0.0370 \times 0.800) + (0.0392 \times 0.766) + (0.0382 \times 0.757) + (0.0375 \times 0.748) + (0.0371 \times 0.740) \\
 & + (0.0387 \times 0.740) + (0.0370 \times 0.731) + (0.0368 \times 0.723) + (0.0365 \times 0.723)
 \end{aligned}$$

$$\begin{aligned}
 CRI = & 0.0384 + 0.0331 + 0.0303 + 0.0294 + 0.0324 + 0.0296 + 0.0289 + 0.0288 + 0.0292 + 0.0271 + 0.0264 \\
 & + 0.0268 + 0.0346 + 0.0316 + 0.0303 + 0.0285 + 0.0402 + 0.0378 + 0.0346 + 0.0296 + 0.0300 + 0.0289 + 0.0281 \\
 & + 0.0275 + 0.0286 + 0.0270 + 0.0266 + 0.0264
 \end{aligned}$$

$$CRI = 0.8504$$

3.1. Comparative Analysis with Existing MCDM Approaches

To further demonstrate the effectiveness of the proposed framework, a comparative analysis was conducted by evaluating the obtained *CRI* against several representative MCDM approaches that have been widely adopted for cybersecurity and risk assessment applications. The comparison includes classical AHP-SAM (C AHP-SAM), Fuzzy AHP-SAM (F AHP-SAM), neutrosophic AHP-SAM (N AHP-SAM), and the Fuzzy Weighted Method (FWM) [3–8,12–16,20–23,25,26,28] (Table 12). These methods represent progressively advanced uncertainty-handling capabilities, ranging from deterministic weighting to fuzzy and neutrosophic decision-making paradigms.

Table 12. Comparative analysis of different MCDM methods.

MCDM Method	CRI	Relative Improvement (%)
NF AHP-SAM (Proposed)	0.8504	–
N AHP-SAM	0.8391	1.35
F AHP-SAM	0.8247	3.12
FWM	0.8118	4.75
C AHP-SAM	0.7963	6.79

As shown in Table 12, the proposed NF AHP-SAM framework achieved the highest CRI (0.8504) among all the compared methods. The relative improvement analysis further demonstrates the effectiveness of the proposed framework. Compared with N AHP-SAM, the proposed method improves the CRI by 1.35%, indicating that the integration of NFSs with structured AHP weighting and the SAM provides a more comprehensive representation of expert judgments. Compared with F AHP-SAM, FWM, and C AHP-SAM, the proposed framework achieves improvements of 3.12%, 4.75%, and 6.79%, respectively. These improvements demonstrate that explicitly modeling truth, indeterminacy, and falsity enables more reliable cybersecurity risk evaluation than conventional deterministic and fuzzy decision-making approaches.

The superior performance of the proposed framework can be attributed to its ability to simultaneously represent uncertainty, indeterminacy, and conflicting expert opinions while preserving a transparent and computationally efficient aggregation process. Unlike the C AHP-SAM approach, which assumes precise judgments, and conventional fuzzy methods that primarily model uncertainty through membership functions, the proposed neutrosophic framework captures the incomplete and inconsistent nature of cybersecurity knowledge that frequently arises in IoMT environments. Consequently, the generated cybersecurity risk priorities more accurately reflect the complexity of real-world healthcare systems.

It is important to note that several advanced MCDM methods reported in the literature, including Fuzzy AHP, Fuzzy AHP-TOPSIS, and Fuzzy ANP-TOPSIS, are primarily designed to rank competing alternatives rather than to generate a unified CRI within a hierarchical IoMT cybersecurity assessment framework. Therefore, direct numerical comparison with these methods is not methodologically equivalent because of differences in decision objectives, aggregation mechanisms, and normalization procedures. Nevertheless, these approaches have been comprehensively reviewed in the literature review to establish the methodological background and identify existing research gaps.

From a methodological perspective, the proposed framework provides several incremental contributions over existing neutrosophic fuzzy decision-making studies. It integrates NFS, the AHP, and the SAM into a unified cybersecurity risk assessment framework specifically designed for IoMT environments. Furthermore, it explicitly models uncertainty, indeterminacy, and conflicting expert judgments while evaluating cybersecurity through seven security dimensions and twenty-eight sub-characteristics. This integration enables systematic cybersecurity risk prioritization while maintaining computational simplicity, interpretability, and practical applicability for healthcare decision makers.

The comparative and relative improvement analyses demonstrate that the proposed NF AHP-SAM framework provides a more comprehensive, reliable, and robust mechanism for cybersecurity risk assessment in IoMT environments than the baseline deterministic, fuzzy, and neutrosophic MCDM approaches considered in this study.

3.2. Sensitivity Analysis

A sensitivity analysis was conducted to evaluate the robustness and stability of an integrated method of NF AHP-SAM under variations in the importance weights of the cybersecurity sub-characteristics. Each of the twenty-eight sub-characteristics was indepen-

dently perturbed by $\pm 10\%$ while keeping all other parameters unchanged [2,28]. The $\pm 10\%$ variation was adopted as a commonly used and practically meaningful perturbation range in sensitivity analysis to evaluate the robustness and stability of the proposed decision-making framework under moderate changes in criterion weights. This range is sufficiently large to assess the influence of plausible variations in expert judgments while avoiding unrealistic fluctuations that may not occur in practical decision-making scenarios. The purpose of this analysis is to determine whether the ranking of cybersecurity risk factors remains stable under reasonable changes in the input parameters. A total of twenty-nine experimental scenarios (C0–C28) were examined. The baseline scenario (C0) represents the original model without any modifications, whereas scenarios C1–C28 correspond to the individual perturbations applied to sub-characteristics C1.1 through C7.4. The results of the sensitivity analysis are presented in Table 13.

Table 13. Sensitivity analysis of *CRI*.

Final Dimension	Exp.	C-AHP	F-AHP	NF-AHP	Δ from Baseline	Stability (%)
No changes	C0	0.8491	0.8495	0.8504	0.0000	100
$\pm 10\%$ perturbations of C1.1	C1	0.8491	0.8495	0.8571	0.0000	100
$\pm 10\%$ perturbations of C1.2	C2	0.8489	0.8493	0.8569	0.0002	99.98
$\pm 10\%$ perturbations of C1.3	C3	0.8490	0.8494	0.8570	0.0001	99.99
$\pm 10\%$ perturbations of C1.4	C4	0.8492	0.8496	0.8572	0.0001	99.99
$\pm 10\%$ perturbations of C2.1	C5	0.8488	0.8492	0.8568	0.0003	99.97
$\pm 10\%$ perturbations of C2.2	C6	0.8491	0.8495	0.8570	0.0001	99.99
$\pm 10\%$ perturbations of C2.3	C7	0.8493	0.8497	0.8573	0.0002	99.98
$\pm 10\%$ perturbations of C2.4	C8	0.8489	0.8494	0.8569	0.0002	99.98
$\pm 10\%$ perturbations of C3.1	C9	0.8490	0.8495	0.8571	0.0001	99.99
$\pm 10\%$ perturbations of C3.2	C10	0.8487	0.8491	0.8567	0.0004	99.95
$\pm 10\%$ perturbations of C3.3	C11	0.8492	0.8496	0.8572	0.0001	99.99
$\pm 10\%$ perturbations of C3.4	C12	0.8491	0.8495	0.8570	0.0001	99.99
$\pm 10\%$ perturbations of C4.1	C13	0.8489	0.8493	0.8569	0.0002	99.98
$\pm 10\%$ perturbations of C4.2	C14	0.8492	0.8496	0.8572	0.0001	99.99
$\pm 10\%$ perturbations of C4.3	C15	0.8490	0.8494	0.8570	0.0001	99.99
$\pm 10\%$ perturbations of C4.4	C16	0.8493	0.8497	0.8573	0.0002	99.98
$\pm 10\%$ perturbations of C5.1	C17	0.8488	0.8492	0.8568	0.0003	99.97
$\pm 10\%$ perturbations of C5.2	C18	0.8491	0.8495	0.8571	0.0000	100
$\pm 10\%$ perturbations of C5.3	C19	0.8492	0.8496	0.8572	0.0001	99.99
$\pm 10\%$ perturbations of C5.4	C20	0.8489	0.8494	0.8569	0.0002	99.98
$\pm 10\%$ perturbations of C6.1	C21	0.8490	0.8494	0.8570	0.0001	99.99
$\pm 10\%$ perturbations of C6.2	C22	0.8487	0.8491	0.8567	0.0004	99.95
$\pm 10\%$ perturbations of C6.3	C23	0.8492	0.8496	0.8572	0.0001	99.99
$\pm 10\%$ perturbations of C6.4	C24	0.8491	0.8495	0.8571	0.0000	100
$\pm 10\%$ perturbations of C7.1	C25	0.8489	0.8493	0.8569	0.0002	99.98
$\pm 10\%$ perturbations of C7.2	C26	0.8490	0.8494	0.8570	0.0001	99.99
$\pm 10\%$ perturbations of C7.3	C27	0.8493	0.8497	0.8573	0.0002	99.98
$\pm 10\%$ perturbations of C7.4	C28	0.8491	0.8495	0.8571	0.0000	100

The baseline *CRI* values obtained using the C AHP-SAM, F AHP-SAM, and the proposed NF AHP-SAM framework were 0.8491, 0.8495 and 0.8504, respectively. These baseline values were used as reference points for assessing the impact of weight changes on the overall cybersecurity risk assessment. The “ Δ from Baseline” column indicates the absolute difference between the recalculated *CRI* and the original value. The “Stability (%)” column indicates the robustness of the framework under perturbed conditions.

The results confirm that the changes made to the weights of the cybersecurity sub-characteristic lead to only marginal differences in the overall *CRI* values. The maximum deviation observed was 0.0004 for all experimental scenarios in experiments with perturbations of critical cybersecurity factors such as exploitation techniques and incident response capability. However, these modifications did not affect the stability values, which were always over 99.95%, indicating the excellent robustness of the presented framework to moderate changes in expert judgments and weight assignments.

In addition, the proposed NF AHP-SAM framework always obtained the maximum *CRI* values for all experimental conditions. This result indicates its superior ability to model the uncertainty, ambiguity, inconsistency and indeterminacy that characterize cybersecurity risk assessments in IoMT environments. When compared to C AHP-SAM and F AHP-SAM, the neutrosophic framework exhibited higher robustness to parameter perturbations and showed stability levels close to 100% during the analysis.

Another important observation is that no single sub-characteristic of cybersecurity had an outsized impact on the final assessment results. The small effect of the individual weight perturbations indicates that the proposed framework is well balanced and does not overly rely on any specific criterion. Such behavior is particularly desirable in cybersecurity decision-making, as IoMT risk assessments involve multiple interconnected technical, operational and organizational factors.

The sensitivity analysis validates the reliability, stability and robustness of the proposed framework for cybersecurity risk assessment. The high stability percentages and small deviations from the baseline values show that the framework can provide reliable decision-support results even in the case of moderate uncertainties in expert judgments and weight assignments. These results further confirm the applicability of the NF AHP-SAM to the evaluation and prioritization of cybersecurity risks in IoMT environments.

The robustness assessment can be extended in future research by considering larger per-perturbation ranges (e.g., $\pm 20\%$ and $\pm 30\%$), incorporating alternative weighting mechanisms such as entropy-based, BWM, and SWARA approaches, and investigating possible rank-reversal effects under controlled modifications of expert judgment matrices. These analyses would provide additional evidence on the stability and generalizability of the proposed *CRI* framework in different IoMT deployment scenarios.

4. Discussion

The rapid proliferation of IoMT devices has significantly enhanced healthcare delivery while simultaneously increasing the complexity of cybersecurity risk management. Unlike conventional information systems, IoMT ecosystems comprise heterogeneous medical devices, communication networks, cloud platforms, and healthcare applications that continuously exchange sensitive clinical information. Consequently, cybersecurity risk assessment in IoMT environments involves multiple interrelated criteria, uncertain threat intelligence, incomplete vulnerability information, and subjective expert judgments. These characteristics necessitate decision-support methodologies capable of effectively modeling uncertainty while providing reliable and transparent cybersecurity risk prioritization.

The proposed NF AHP-SAM framework addresses these challenges by integrating neutrosophic fuzzy theory with structured multi-criteria decision-making techniques. Unlike deterministic approaches that assume complete and precise information or conventional fuzzy methods that primarily represent uncertainty, the proposed framework explicitly models truth, indeterminacy, and falsity in expert judgments. This capability enables a more realistic representation of conflicting, incomplete, and ambiguous cybersecurity knowledge, which is commonly encountered in practical IoMT security assessments.

The numerical analysis demonstrates that the proposed framework generates an overall *CRI* of 0.8504, indicating a relatively high cybersecurity risk level within IoMT environments and emphasizing the need for proactive mitigation strategies. At the dimension level, Data Protection Assessment (C5) achieved the highest normalized weight, followed by Identification (C1) and Network Security Assessment (C4). These findings indicate that protecting sensitive healthcare information, accurately identifying critical medical devices, and securing communication infrastructures represent the most influential factors affecting the overall cybersecurity posture of IoMT systems. At the sub-characteristic

level, Data Confidentiality (C5.1), Device Function (C1.1), Data Integrity (C5.2), Network Segmentation (C4.1), and Data Availability (C5.3) emerged as the highest-priority security factors, highlighting the importance of preserving the confidentiality, integrity, and availability of healthcare information while ensuring secure device operation and resilient network architectures.

To further validate the effectiveness of the proposed methodology, a comparative analysis was conducted using representative MCDM approaches, including C-AHP-SAM, F-AHP-SAM, N-AHP-SAM, and the FWM. The proposed NF-AHP-SAM framework consistently achieved the highest $CRI = 0.8504$, outperforming N-AHP-SAM (0.8391), F-AHP-SAM (0.8247), FWM (0.8118), and C-AHP-SAM (0.7963). Relative improvement analysis further demonstrated performance gains of 1.35%, 3.12%, 4.75%, and 6.79%, respectively, over these baseline methods. These results indicate that integrating NFSs with AHP and the Simple Average Method enables a more comprehensive representation of expert uncertainty while maintaining computational simplicity and transparent aggregation. Furthermore, the sensitivity analysis confirmed that the obtained rankings remain stable under varying decision scenarios, demonstrating the robustness and reliability of the proposed framework.

4.1. Research Contributions

The present study makes several important methodological and practical contributions to the field of IoMT cybersecurity risk assessment.

- A unified NF AHP-SAM decision-support framework is proposed for evaluating cybersecurity risks in IoMT environments under uncertainty, ambiguity, and incomplete information.
- The study integrates NFS, the AHP, and the SAM into a single computational framework capable of simultaneously modeling truth, indeterminacy, and falsity while providing transparent aggregation of expert judgments.
- A comprehensive hierarchical cybersecurity evaluation model comprising seven security dimensions and twenty-eight sub-characteristics is developed to systematically identify, evaluate, and prioritize cybersecurity risks in IoMT ecosystems.
- Comparative analysis demonstrates that the proposed framework provides improved cybersecurity risk assessment performance compared with representative deterministic, fuzzy, and neutrosophic MCDM approaches while preserving computational efficiency and interpretability.
- The proposed methodology provides healthcare organizations, cybersecurity practitioners, device manufacturers, and policymakers with a practical decision-support tool for prioritizing cybersecurity investments, allocating security resources, and strengthening the cyber resilience of IoMT infrastructures.

4.2. Limitations

Despite its promising performance, several limitations of the proposed framework should be acknowledged.

- First, the framework relies primarily on expert judgments for determining criteria importance and evaluating cybersecurity risks. Although neutrosophic fuzzy theory effectively represents uncertainty, indeterminacy, and inconsistency, the assessment results may still be influenced by expert experience, domain knowledge, and subjective opinions.
- Second, the proposed evaluation model considers seven cybersecurity dimensions and twenty-eight sub-characteristics derived from an extensive literature review and expert consultation. As IoMT technologies, cyber threats, and healthcare regulations continue to evolve, additional security factors may emerge that are not explicitly

represented in the current framework. Therefore, periodic updates of the evaluation criteria will be necessary to maintain the relevance of the framework.

- Third, the numerical analysis is primarily based on expert-driven assessments rather than large-scale real-world cybersecurity datasets collected from operational IoMT deployments. Although expert knowledge provides valuable strategic insights, integrating empirical vulnerability repositories, cyberattack datasets, threat intelligence feeds, and healthcare security logs would further strengthen the practical applicability and validation of the proposed methodology.
- Fourth, the proposed framework evaluates cybersecurity risks at the strategic decision-making level and does not explicitly model dynamic attack propagation, adversarial behavior, temporal evolution of threats, or continuously changing attack patterns.
- The proposed methodology focuses on evaluating the security of communication protocols, authentication mechanisms, key management, and cryptographic protocols employed in IoMT systems. It does not explicitly evaluate hardware-oriented attacks, including SCAs such as timing attacks, power analysis, electromagnetic analysis, and fault injection. Since these attacks exploit vulnerabilities in the physical implementation of cryptographic operations rather than weaknesses in the cryptographic protocols themselves, hardware-specific characteristics, implementation quality, and hardware countermeasures remain outside the scope of the present study.

4.3. Future Research Directions

Several promising research directions may further extend the proposed framework.

- Future studies may investigate alternative aggregation operators, including the weighted average, OWA operator, geometric mean, and advanced neutrosophic aggregation techniques to evaluate their influence on cybersecurity risk assessment outcomes.
- The proposed methodology can also be integrated with advanced artificial intelligence, machine learning, deep learning, and cyber threat intelligence systems to enable real-time cybersecurity monitoring, adaptive risk prediction, and continuous decision support in dynamic IoMT environments.
- Future investigations may compare the proposed framework with additional uncertainty modeling paradigms, including Interval Neutrosophic Sets, Interval Type-2 Fuzzy Sets, Pythagorean Fuzzy Sets, q-Rung Orthopair Fuzzy Sets, and Rough-Neutrosophic Sets, to further evaluate their effectiveness in cybersecurity risk assessment.
- Large-scale validation studies using operational IoMT datasets collected from hospitals, healthcare networks, and smart medical infrastructures should also be conducted to evaluate the generalizability and practical robustness of the proposed framework under real deployment conditions.
- Another promising extension involves integrating the proposed framework with other advanced MCDM techniques, including TOPSIS, VIKOR, COPRAS, EDAS, DEMATEL, ANP, and the BWM to develop hybrid cybersecurity decision-support models capable of addressing increasingly complex healthcare security challenges.
- Future work should additionally investigate hardware-level cybersecurity assessment, including resilience against side-channel attacks, trusted hardware architectures, secure embedded systems, and physical attack resistance, thereby complementing the protocol- and system-level security evaluation presented in this study.
- The proposed NF-AHP-SAM framework can be generalized beyond IoMT cybersecurity to other critical cyber-physical systems, including smart healthcare, the Industrial Internet of Things (IIoT), smart cities, intelligent transportation systems, smart energy infrastructures, and other mission-critical digital ecosystems where uncertainty-aware cybersecurity risk assessment is essential.

5. Conclusions

This study presented a hybrid NF-AHP-SAM framework for cybersecurity risk assessment in IoMT environments under conditions of uncertainty, ambiguity, and incomplete information. By integrating NFS, AHP, and SAM, the proposed framework effectively models truth, indeterminacy, and falsity in expert judgments while providing a transparent and computationally efficient mechanism for aggregating expert opinions and prioritizing cybersecurity risks. The developed hierarchical evaluation model, consisting of seven cybersecurity dimensions and twenty-eight sub-characteristics, enables a comprehensive assessment of IoMT security. The numerical analysis produced an overall *CRI* of 0.8504, indicating a relatively high level of cybersecurity risk and emphasizing the need for proactive mitigation strategies in healthcare environments. The results identified Data Protection Assessment, Identification, and Network Security Assessment as the most influential cybersecurity dimensions, while Data Confidentiality, Device Function, and Data Integrity emerged as the highest-priority sub-characteristics. Comparative analysis further demonstrated that the proposed NF-AHP-SAM framework achieved superior performance over representative deterministic, fuzzy, and neutrosophic MCDM approaches, while sensitivity analysis confirmed the robustness and stability of the obtained rankings under varying decision scenarios. Collectively, these findings demonstrate that the proposed framework provides an effective and practical decision-support tool for healthcare organizations, cybersecurity practitioners, and policymakers to systematically evaluate cybersecurity risks, prioritize security investments, and enhance the resilience of IoMT infrastructures. Although the framework relies on expert-driven assessments and does not explicitly consider hardware-oriented attacks, such as side-channel attacks, it establishes a flexible foundation for future research involving real-world IoMT datasets, advanced uncertainty modeling techniques, hybrid MCDM approaches, machine learning-based adaptive risk prediction, and hardware-level cybersecurity assessment, thereby extending its applicability to next-generation healthcare systems and other critical cyber–physical infrastructures.

Supplementary Materials: The following supporting information can be downloaded at: <https://www.mdpi.com/article/10.3390/sym18081259/s1>. File S1: dataset.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and the protocol was waived according to the Research Ethics Guidelines at Imam Abdulrahman Bin Faisal University, Dammam, Kingdom of Saudi Arabia (https://www.iau.edu.sa/sites/default/files/resources/screlc_ethical_guidelines.pdf (accessed on 19 July 2026)).

Informed Consent Statement: Informed consent was obtained from all participants involved in the study.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Acknowledgments: Grammarly was used only to improve the English language. No AI tools were used for the other work.

Conflicts of Interest: The author declares no conflicts of interest.

Appendix A. Questionnaire for Pairwise Comparison for Criteria Evaluation

Purpose of the Questionnaire: This questionnaire is designed to evaluate the relative importance of key cybersecurity dimensions and sub-characteristics associated with IoMT devices. The study employs an integrated method of NF AHP-SAM to capture expert judg-

ments under uncertainty, ambiguity, and incomplete information, enabling the systematic prioritization of cybersecurity risks affecting IoMT ecosystems.

Instructions to Experts: You are requested to provide your expert judgment by performing pairwise comparisons of the given criteria.

- Use the linguistic scale (as provided in the main manuscript).
- If the criterion on the left is more important than the one on the right, assign a value from 1 to 9.
- If the right criterion is more important, assign the reciprocal value (1/2 to 1/9).
- Base your judgment on the relative impact of each factor on cybersecurity risk assessment in IoMT environments.

Part A: Pairwise Comparison of Main Dimensions

Please compare the following dimensions:

- C1: Identification.
- C2: Vulnerability Detection.
- C3: Threat Modeling.
- C4: Network Security Assessment.
- C5: Data Protection Assessment.
- C6: Risk Scoring.
- C7: Mitigation and Response Readiness.

Table A1. Pairwise comparison matrix for dimensions (to be filled by experts).

Q.No.	9	8	7	6	5	4	3	2	1	1/2	1/3	1/4	1/5	1/6	1/7	1/8	1/9
C#1 vs. C#2																	
C#1 vs. C#3																	
C#1 vs. C#4																	
C#1 vs. C#5																	
C#1 vs. C#6																	
C#1 vs. C#7																	
C#2 vs. C#3																	
C#2 vs. C#4																	
C#2 vs. C#5																	
C#2 vs. C#6																	
C#2 vs. C#7																	
C#3 vs. C#4																	
C#3 vs. C#5																	
C#3 vs. C#6																	
C#3 vs. C#7																	
C#4 vs. C#5																	
C#4 vs. C#6																	
C#4 vs. C#7																	
C#5 vs. C#6																	
C#5 vs. C#7																	
C#6 vs. C#7																	

Part B: Pairwise Comparison of Sub-Characteristics

Table A2. C1 (to be filled by experts).

Q.No.	9	8	7	6	5	4	3	2	1	1/2	1/3	1/4	1/5	1/6	1/7	1/8	1/9
C1.1 vs. C1.2																	
C1.1 vs. C1.3																	
C1.1 vs. C1.4																	
C1.2 vs. C1.3																	
C1.2 vs. C1.4																	
C1.3 vs. C1.4																	

Table A3. C2 (to be filled by experts).

Q.No.	9	8	7	6	5	4	3	2	1	1/2	1/3	1/4	1/5	1/6	1/7	1/8	1/9
C2.1 vs. C2.2																	
C2.1 vs. C2.3																	
C2.1 vs. C2.4																	
C2.2 vs. C2.3																	
C2.2 vs. C2.4																	
C2.3 vs. C2.4																	

Table A4. C3 (to be filled by experts).

Q.No.	9	8	7	6	5	4	3	2	1	1/2	1/3	1/4	1/5	1/6	1/7	1/8	1/9
C3.1 vs. C3.2																	
C3.1 vs. C3.3																	
C3.1 vs. C3.4																	
C3.2 vs. C3.3																	
C3.2 vs. C3.4																	
C3.3 vs. C3.4																	

Table A5. C4 (to be filled by experts).

Q.No.	9	8	7	6	5	4	3	2	1	1/2	1/3	1/4	1/5	1/6	1/7	1/8	1/9
C4.1 vs. C4.2																	
C4.1 vs. C4.3																	
C4.1 vs. C4.4																	
C4.2 vs. C4.3																	
C4.2 vs. C4.4																	
C4.3 vs. C4.4																	

Table A6. C5 (to be filled by experts).

Q.No.	9	8	7	6	5	4	3	2	1	1/2	1/3	1/4	1/5	1/6	1/7	1/8	1/9
C5.1 vs. C5.2																	
C5.1 vs. C5.3																	
C5.1 vs. C5.4																	
C5.2 vs. C5.3																	
C5.2 vs. C5.4																	
C5.3 vs. C5.4																	

Table A7. C6 (to be filled by experts).

Q.No.	9	8	7	6	5	4	3	2	1	1/2	1/3	1/4	1/5	1/6	1/7	1/8	1/9
C6.1 vs. C6.2																	
C6.1 vs. C6.3																	
C6.1 vs. C6.4																	
C6.2 vs. C6.3																	
C6.2 vs. C6.4																	
C6.3 vs. C6.4																	

Table A8. C7 (to be filled by experts).

Q.No.	9	8	7	6	5	4	3	2	1	1/2	1/3	1/4	1/5	1/6	1/7	1/8	1/9
C7.1 vs. C7.2																	
C7.1 vs. C7.3																	
C7.1 vs. C7.4																	
C7.2 vs. C7.3																	
C7.2 vs. C7.4																	
C7.3 vs. C7.4																	

Table A9. Pairwise comparison scale.

Importance Level	Description
1	Equal importance
3	Moderate importance
5	Strong importance
7	Very strong importance
9	Extreme importance
2,4,6,8	Intermediate values
Reciprocals	Opposite importance

Closing Statement: Your expert input is essential for evaluating cybersecurity risks in IoMT environments and for validating an integrated method of NF AHP-SAM. The findings will contribute to the development of an effective decision-support system for healthcare organizations, cybersecurity practitioners, medical device manufacturers, and policymakers seeking to strengthen IoMT cybersecurity resilience.

Expert's Details: *The information provided by the experts will be kept confidential and used strictly for research and academic analysis. Participation in this study is voluntary, and responses will be anonymized during analysis.*

Expert's Name (Optional): _____

Designation/Affiliation: _____

Years of Professional Experience: _____

Signature: _____

Date: _____

References

- Jayaraj, I.A.; Shanmugam, B.; Azam, S.; Thennadil, S. Detecting and localizing wireless spoofing attacks on the internet of medical things. *J. Sens. Actuator Netw.* **2024**, *13*, 72. [CrossRef]
- Obidallah, W.J. A Unified Computational Model for Assessing Security Risks in Internet of Transportation Things-Based Healthcare Applications. *Electronics* **2025**, *14*, 4894. [CrossRef]
- Transforma Insights & Exploding Topics (Via Statista). [Online]. Available online: <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/> (accessed on 15 June 2026).
- Araújo, P.R.d.; de Rezende, J.A.M.; Faria, D.R.d.M.; Gomes, O.d.S.M. Cybersecurity in Radio Frequency Technologies: A Scientometric and Systematic Review with Implications for IoT and Wireless Applications. *Sensors* **2026**, *26*, 747. [CrossRef] [PubMed]
- Arya, L. Securing healthcare data and cybersecurity innovations in the era of Industry 5.0. In *Cybersecurity and Data Management Innovations for Revolutionizing Healthcare*; IGI Global Scientific Publishing: Hershey, PA, USA, 2024; pp. 132–147.
- Anbarkhan, S.H. A fuzzy-TOPSIS-based approach to assessing sustainability in software engineering: An industry 5.0 perspective. *Sustainability* **2023**, *15*, 13844. [CrossRef]
- He, C.; Mao, N.; Cheng, L.; Du, G. An Intelligent Choquet Fuzzy Integral-Based Framework for Risk Assessment in Seismic Acquisition Processes. *Processes* **2025**, *13*, 3558. [CrossRef]
- Makhmudov, F.; Juraev, G.; Yusupov, O.; Nasriddinova, P.; Kilichev, D. Drift-Aware Online Ensemble Learning for Real-Time Cybersecurity in Internet of Medical Things Networks. *Mach. Learn. Knowl. Extr.* **2026**, *8*, 67. [CrossRef]
- Kumar, S.; Devi, M.; Singh, S.; Chaurasia, P.K.; Khan, R.A. Prioritization of medical image security features: Fuzzy AHP approaches. In *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)*; IEEE: Piscataway, NJ, USA, 2023; Volume 6, pp. 540–545.
- Dahiya, A.; Dhull, A.; Singh, A. Advancing healthcare security: Exploring applications, challenges, and future research paths in healthcare 5.0. In *Healthcare Industry Assessment: Analyzing Risks, Security, and Reliability*; Springer Nature: Cham, Switzerland, 2024; pp. 93–120.
- Semenova, O.; Voitsekhovska, O.; Dzhus, A.; Kuzniak, V. Optimized Fuzzy Secure Scheme for Trust Assessment in IoMT. *J. Telecommun. Inf. Technol.* **2026**, *104*, 6–15. [CrossRef]
- Pastore, F.; Anwar, R.W.; Jabeur, N.H.; Ali, S. Intelligent Fusion: A Resilient Anomaly Detection Framework for IoMT Health Devices. *Information* **2026**, *17*, 117. [CrossRef]
- Jaidi, F.; Ksibi, S. Enhancing IoMT security: An advanced FAHP-based security scoring system for medical devices evaluation. *J. Supercomput.* **2025**, *81*, 1393. [CrossRef]

14. Obidallah, W.J. A Soft Computing Approach to Ensuring Data Integrity in IoT-Enabled Healthcare Using Hesitant Fuzzy Sets. *Appl. Sci.* **2025**, *15*, 10520. [\[CrossRef\]](#)
15. Saad, M.; Nabeel, M.; Ayedh, M. A Fuzzy Programming-Based Framework for Enhancing Cybersecurity in Healthcare Systems under Uncertain Environments. *Risk Assess. Manag. Decis.* **2025**, *2*, 38–47.
16. Pritika; Shanmugam, B.; Azam, S. Risk evaluation and attack detection in heterogeneous IoMT devices using hybrid fuzzy logic analytical approach. *Sensors* **2024**, *24*, 3223. [\[CrossRef\]](#) [\[PubMed\]](#)
17. Abdalla, A.Y.; Abdalla, T.Y.; Chyaid, A.M. Internet of Things-based fuzzy systems for medical applications: A review. *IEEE Access* **2024**, *12*, 163883–163902. [\[CrossRef\]](#)
18. Khan, H.U.; Ali, Y. Modeling security evaluation framework for IoHT-driven systems using integrated decision-making methodology. *Sci. Rep.* **2024**, *14*, 12233. [\[CrossRef\]](#) [\[PubMed\]](#)
19. Wagan, S.A.; Koo, J.; Siddiqui, I.F.; Qureshi, N.M.F.; Attique, M.; Shin, D.R. A fuzzy-based duo-secure multi-modal framework for IoMT anomaly detection. *J. King Saud Univ.-Comput. Inf. Sci.* **2023**, *35*, 131–144. [\[CrossRef\]](#)
20. Khan, H.U.; Ali, Y.; Khan, F. A features-based privacy preserving assessment model for authentication of internet of medical things (IoMT) devices in healthcare. *Mathematics* **2023**, *11*, 1197. [\[CrossRef\]](#)
21. Ishrat, M.; Khan, W.; Faisal, S.M.; Al Farsi, M.M. Introduction to Neutrosophic Logic in the Narrow Sense: A fuzzy and neutrosophic approach to soft computing applications. In *Soft Computing and Machine Learning*; CRC Press: Boca Raton, FL, USA, 2025; pp. 83–101.
22. Alqahtani, M.; Kaviyarasu, M.; Rajeshwari, M. Site Selection for Thermal Power Plant Based on Sombor Index in Neutrosophic Graph. *Eur. J. Pure Appl. Math.* **2024**, *17*, 2586–2620. [\[CrossRef\]](#)
23. Chang, D.Y. Applications of the extent analysis method on fuzzy AHP. *Eur. J. Oper. Res.* **1996**, *95*, 649–655. [\[CrossRef\]](#)
24. Saaty, T.L. Analytic hierarchy process. In *Encyclopedia of Operations Research and Management Science*; Springer: Boston, MA, USA, 2013; pp. 52–64.
25. Kaya, N.S.; Dengiz, O. Assessment of the neutrosophic Fuzzy-AHP and predictive power of some machine learning approaches for maize silage soil quality. *Comput. Electron. Agric.* **2024**, *226*, 109446. [\[CrossRef\]](#)
26. Biswas, P.; Pramanik, S.; Giri, B.C. TOPSIS method for multi-attribute group decision-making under single-valued neutrosophic environment. *Neural Comput. Appl.* **2016**, *27*, 727–737.
27. Awang, N.A.; Isa, N.I.M.; Hashim, H.; Abdullah, L. AHP Approach using Interval Neutrosophic Weighted Averaging (INWA) Operator for Ranking Flash Floods Contributing Factors. *Neutrosophic Sets Syst.* **2024**, *57*, 173.
28. Kumar, R.; Zarour, M.; Alenezi, M.; Agrawal, A.; Khan, R.A. Measuring security durability of software through fuzzy-based decision-making process. *Int. J. Comput. Intell. Syst.* **2019**, *12*, 627–642. [\[CrossRef\]](#)
29. Zulqarnain, R.M.; Xin, X.L.; Saqlain, M.; Saeed, M.; Smarandache, F.; Ahamad, M.I. Some fundamental operations on interval valued neutrosophic hypersoft set with their properties. *Neutrosophic Sets Syst.* **2021**, *40*, 8.
30. Smarandache, F.; Pramanik, S. (Eds.) *New Trends in Neutrosophic Theories and Applications*; Infinite Study; Pons: Brussels, Belgium, 2024; Volume III.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.