applied sciences

MDPI

Article

Towards Design and Development of Security Assessment Framework for Internet of Medical Things

Fahad A. Alzahrani [1], Masood Ahmad [2] and Md Tarique Jamal Ansari [2,*]

[1] Computer Engineering Department, College of Computer and Information Systems, Umm Al-Qura University, Makkah 21955, Saudi Arabia
[2] Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow 226025, Uttar Pradesh, India
* Correspondence: tjtjansari@gmail.com

Abstract: The majority of medical equipment in use today does not have built-in security features. As a result, whether linked to a hospital system or the cloud, these devices' built-in weaknesses make them vulnerable to a variety of cyberattacks. In hospitals and clinics, hackers can breach equipment, manipulate data, and disrupt facilities, putting patients' health as well as their lives in jeopardy. A professional can manage cybersecurity threats by lowering the attack surface of the system. Security analysis, whether as a means to detect possible vulnerabilities that can be exploited by attackers or as a means to prevent cyberattacks, plays an important role in risk mitigation. In addition, throughout the pre-market and post-market phases, security checks are required. This study presents a paradigm for incorporating security check concepts into medical device design and development and healthcare big data security. The security of devices and healthcare data is tested by the integrated fuzzy AHP-TOPSIS method. After the security check of devices, with the parameters security-checked for data, the algorithm is designed and implemented. As a result, the appropriate customized security controls are prompted in order to impede the attack.

Keywords: medical device; healthcare; big data; security; cybersecurity; AHP; TOPSIS

check for updates

Citation: Alzahrani, F.A.; Ahmad, M.; Ansari, M.T.J. Towards Design and Development of Security Assessment Framework for Internet of Medical Things. *Appl. Sci.* **2022**, *12*, 8148. https://doi.org/10.3390/app12168148

Academic Editor: Vincent A. Cicirello

Received: 30 June 2022
Accepted: 11 August 2022
Published: 15 August 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

In the medical profession, technological advancements have brought both opportunities and obstacles. Medical devices and healthcare data have progressed from stand-alone to networked arrangements [1,2]. In the healthcare industry, the ever-expanding web of linked devices is increasing at a rapid pace and across a wide range of industries. Nowadays, the normal hospital room has 15 to 20 linked pieces of health equipment, with large hospitals having up to 85,000 [3]. Integrating a healthcare Cyber-Physical System (CPS) might significantly reduce clinical mistakes as well as expenses, enhance patient care as well as intervention quality, strengthen workflow productivity, and lower the workload of healthcare workers. Moreover, it reveals flaws that could make healthcare systems vulnerable to cyberattacks [4].

The proliferation of networked equipment is altering the cyber threat environment. Threats are becoming more prevalent and complex. A malicious user may use wireless techniques to inject instructions that change the capabilities of gadgets or jam wireless indicators to prevent device accessibility as well as therapeutic delivery [5]. Medical supplies can be used in cyber warfare to target public officials who use them, as well as potentially trigger significant health issues or fatalities [6]. Medical equipment cybersecurity weaknesses cause approximately 100 patients to be affected each year. Susceptible public healthcare big data are stored in healthcare network systems, which are guarded by security and privacy regulations. Moreover, network-connected healthcare systems are often highly susceptible to privacy and security threats than general-purpose network servers as well as end devices due to the wide range of equipment.

The calibration and maintenance of medical equipment are normally the responsibility of biomedical or clinical engineering departments. Security, healthcare data protection, and cleanup are tough for them because they are not IT organizations. Medical devices have extensive product life cycles and rely on operating systems from previous generations. Fixing and updating such systems is not always feasible, and when it is, configuration can be challenging, possibly requiring acceptance testing. Medical device manufacturers, not device owners, ought to be responsible for security fixes for system control as well as setup validation [7]. Manufacturers' lack of access limits security and data protection improvements, as well as quick solutions. Because embedded devices have limited memory, manufacturers frequently employ modified versions of standard operating systems.

As a result, applying software patches and security solutions is difficult. To decrease training costs, most healthcare professionals prefer to employ a single model and manufacturer. As a result, a uniform environment will be formed, allowing security breaches to spread quickly throughout systems.

Vulnerabilities in medical devices pose a threat to both data and patients. In the healthcare industry, the utilization, as well as the incorporation, of wired and wireless networked electronic devices has raised the danger of cyberattacks. The majorities of these devices have open TCP/UDP docks and enable protocols such as TFTP, FTP, and Telnet, which are susceptible to assaults by default [8]. Techniques such as ICMP and NMAP should be used to request device profiles, but they will quit functioning if they are exposed to multipath network activity produced by worms, viruses, and other malware. Medical tools are also very seldom modified or retired from service. The four categories of cyberattacks on medical equipment are remote, physical by authorized individuals, physical by unauthorized individuals, and physical by criminal activities [9]. Wireless-based attacks such as jamming, eavesdropping, replay, and injection can compromise medical devices [10]. The likelihood of software vulnerabilities has increased as a result of the large number of software applications in medical equipment [11]. For example, arbitrary code execution due to a buffer overflow vulnerability, inadequate authentication method, unsuitable credential storage, and unauthorized firmware updates due to improper usage of the Cyclic Redundancy Check were discovered in Hanna et al.'s research [12].

Insiders, outsiders, and natural phenomena can all pose a threat to medical devices, which can be inadvertent or intentional. Threats are classed as passive or active, according to Arney et al. Information collection, interception, and the sniffing of network data are examples of passive threats. Intense attacks include functional coverage disturbance, social manipulation, data leakage, spoofing or identity fraud, spoofing, denial of service, harmful programs, theft of intellectual property, physical harm, and backdoors, as well as the possible loss of patient records.

The creation of advanced CPSs has shifted the design of medical equipment from passive to active devices, which also include intelligent analytic systems with sensing devices [13,14]. Healthcare equipment consists of implantable medical devices (IMDs) as well as wearable medical equipment with wireless transmission functionality. IoMT (Internet of Medical Things) is also linked to the cloud as well as a CPS. Various communication methods are used in CPS applications, including diverse protocols and wired and wireless technologies. Wireless communication is widely employed in medical devices. Medical Implant Communication Service (MICS) signals are used by IMDs, while body area network (BAN) signals, for example, Bluetooth and ZigBee, are used by wearable devices [15]. Impersonation, eavesdropping, and jamming are the most common security vulnerabilities in wireless communication, all of which can be used to undermine the healthcare CPS [16]. Healthcare-related CPSs, for example, IMDs, BANs, and wearable equipment, play a vital role [5] because of their low processing capability, communication complexity, and limited battery life, privacy, and security. The level of security in any system varies depending on the sensitivity of the information and the control system. Because of insufficient standard interfaces and communication protocols, designing, developing, and implementing a viable CPS in application fields such as healthcare present a number

of challenges and limitations [17]. A CPS in the healthcare setting faces issues such as software reliability, medical equipment suitability, data retrieval, technology demonstrator architecture, advanced query processing, privacy and security, and system feedback [18,19]. During data storage, processing, extraction, and reversal to the CPS, a security threat always persists. Lack of network security, ransomware, device vulnerabilities, applications, fake data generation, unauthorized changes in data, and data cleaning problems are all challenges for healthcare big data.

Ransomware, malware, and crypto-jacking are some of the most serious dangers to medical devices and healthcare data [13]. Ransomware is among the highly widespread dangers, compromising healthcare information as well as hindering users' or medical personnel's access to their system unless a large sum of money (a ransom) is paid in exchange for access. If the demanded ransom is not paid in a timely manner, the data may be automatically deleted. More than 78 percent of medical suppliers have been hit by ransomware, spyware, or even both in the last year. Crypto-jacking permits a vulnerable device's computing power to be used to mine cryptocurrency, shortening its lifespan and putting patient as well as medical care information at risk. To avoid or reduce potential cyber threats to medical equipment, vulnerabilities in medical devices and healthcare data generated by the devices must be addressed. As a result, at all stages of the device's data processing lifecycle, a proactive strategy is required. An Attack Surface Reduction technique is presented in this study. The following are the contributions of this research project.

a. A novel security framework for interconnected healthcare devices as well as the patient records they produce.
b. Categorization of attack vectors as well as the implementation of appropriate security control mechanisms to mitigate or completely prevent future attacks.
c. An explanation of how and why the suggested solution would handle medical equipment threats early in product development, before security flaws are taken advantage of, as well as data security techniques to improve data protection.

The rest of this research is laid out as follows. Section 2 discusses relevant efforts on protection strategies in medical equipment. Section 3 gives a high-level introduction to the Attack Surface Reduction structure for a medical equipment strategy. Section 4 shows the implementation and findings. Section 5 presents a discussion of the research findings. Finally, Section 6 is dedicated to concluding remarks and future research directions.

2. Related Works

Sanaz et al. [20] developed a framework for detecting cyberattacks on medical devices that are connected to the internet. The researchers worked on reducing threats by the design scheme in this framework. To identify attacks on networked devices, the authors applied a decision tree approach. Halperin et al. [21] described a technique that uses cryptographic-based authentication and key exchange to prevent unwanted access to patients' IMDs. Instead of using batteries, this system uses an external radio frequency. In wearable and implantable devices, out-of-band (OBB) verification via extra channels is used [5]. In the body sensor network, biometrics was also employed to secure communication (BSN). In another study, Gollakota et al. [22] proposed outer wearable equipment (the shield) that can be used to jam signals and commands delivered to an IMD by an unauthorized person. Their design obstructs others from decoding the IMD's communications. They can be decoded by the shield on its own. It also allows for the jamming of unapproved commands, such as those that attempt to change the shield's specific communications. After being applied in a radio application, it was evaluated with commercial IMDs. Hackers gain access to networks by exploiting virtual functionality used by remote physicians as well as patients' devices. As a consequence, manufacturers must deactivate remote management functionality as well as restrict it from obtaining measurements and audit trails, reducing the device's functionality [23]. Mitchell and Chen [24] proposed an IDS method that is premised on behavior-rule specifications for recognizing sensing devices that threaten the

lives of patients. They suggested medical devices that could be utilized independently. Xu et al. [25] developed IMDGuard to protect against jamming and spoofing attacks. Hayajneh et al. [26] suggested a method established on the basis of the Rabin verification algorithm to improve the signature signing procedure and prevent unauthenticated as well as distant orders from being sent to patients' IMDs. Guo et al. [27] made use of the e-Health system's dispersed structure, allowing patients and physicians to complete authentication. Despite having higher computing costs and communication resources, the suggested attribute-based verification arrangement framework, known as PAAS, is considered to maintain advanced levels of privacy on attributes as well as attribute standards.

Using extensive chaotic maps, Li et al. [28] established a secure authentication and authorization strategy for a cloud-oriented wireless body area network (WBAN) mechanism. Before disseminating the acquired health items, this scheme encrypts them. This approach can be used to authenticate patients in medical care systems. For wireless sensor networks, Lounis et al. [29] devised an access regulator system focused on ciphertext policy attribute-based encryption (CP-ABE). This method reduced administrative overhead as well as encryption and decryption times. This model is fine-grained and defines scalability and efficiency. Gao and Thamilarasu [30] created feature sets for IMD devices that were examined using three distinct algorithms: decision trees, Support Vector Machine (SVM), and K-means. A clustering method based on k-anonymity was presented by Liu and Li [31]. The most similar records are delegated to the same groupings, making sure that identification privacy is maintained. The Euclidean distance is used to determine the correlation between two records, with the guidelines set according to the prescribed standards. A clustering algorithm predicated on k was proposed by Liu and Li [32,33]. Records that are often the most comparable are grouped together, guaranteeing that identification privacy is preserved. The Euclidean distance is used to calculate the similarity between the two records, with the parameters specified according to the actual demand. As a result, further research is needed to mitigate or prevent cyberattacks on this type of attack surface. In addition, intrusions of security measures used in public healthcare CPS implementations have been observed, illustrating their lack of adequacy in securing data as well as communication. Medical equipment is susceptible to attacks, requiring the creation of a secure system. The objective is to develop a system that provides both safety and confidentiality. Only authorized personnel can obtain, recognize, and configure gadgets, whereas privacy guarantees that personal data on devices are kept private.

Well-protected medical equipment necessitates precise security methods that take into account threat landscape changes. All possible attack layers within the medical equipment setting should be assessed throughout the planning stage. In the advancement of clinical equipment, security is the most essential requirement. However, according to Vora and Schaeffer [8], access management, network searching, threat decrease, the underlying basis of trust, cryptographic signature, encryption techniques, and software updates, among many other security measures, can be utilized to either prevent or mitigate the destruction of medical equipment. All of these methods cannot be implemented on a single system. According to the management of risk, several processes can be combined to provide strong coverage against virtual risks. The proposed method has the advantage of detecting and neutralizing insider attackers who have more information about the medical equipment, whereas Gao and Thamilarasu's [30] method failed to do so.

Sun et al. [13] suggested a blockchain-based methodology to secure storage and access of medical data. J. Sun combined the hash function with the blockchain for the verification of the user's authenticity. With this technique, the overall security of electronic medical data is improved, and it allows for the secure storage of data and the authentication of data. Ari et al. [34] proposed a honey encryption-based technique for the security of healthcare data. The authors first encrypt the message using honeycomb-based encryption to secure data from brute force attacks by producing ciphertexts when attackers want to decrypt the data with incorrect keys, yielding feasible gazing plaintexts. Kapil et al. [35] suggested a hybrid methodology for healthcare big data encryption. In their work, they used an

attribute-based honey encryption technique for securing large data sets. In this work, first, the authors encrypt the data using the attribute-based technique, and then they impose the honey encryption technique for another encryption. This hybrid methodology improves the security of healthcare data overall and protects the data from brute force attacks and unwanted access. Yang et al. [36] proposed a hoop-based cloud data security technique. The authors developed a novel encryption technique that is a combination of three different techniques. This triple encryption technique provides very strong data encryption and security. With this technique, it is very difficult for hackers to find the decryption key. This is novel research in big data security.

Ultimately, the majority of the suggested works define the established solution(s) by utilizing post-deployment variables such as architectures, as well as responses from existing subscribers, which necessitates technical expertise that most interested IoMT parties lack. As a result, we introduce the Internet of Medical Things Security evaluation approach, a fuzzy logic-based framework that employs a comprehensive collection of evaluation characteristics covering all IoMT situations as well as stakeholders' selection of alternatives. The work is significant because it enables stakeholders to conveniently evaluate as well as start comparing security and privacy variables in any IoMT solution from their point of view and also in accordance with their security measures. This is significant since stakeholders frequently have various security objectives based on their resources, tolerance for risk, and so on. The proposed framework enables participants to make well-informed judgments when selecting secure IoMT alternatives or enhancing the security of existing approaches.

3. Security Assessment of IoMT

3.1. Types of Attacks and Vectors

According to Yaqoob et al. [11], the various attack routes that cause security infringements are as follows.

(a) Human attack surface: On the human threat landscape, internal threats, forgery, and social threats such as phishing, as well as psychological manipulation, are all probable. Any unintended or malignant activity by a validated insider that could also bypass the platform and compromise its security is included.
(b) Communication protocol attack surface: DoS, man-in-the-middle, and the spoofing of threats can all be carried out using communication systems.
(c) Physical attack surface: Heuristic analysis, equipment attacks, side-channel threats, fraudulent USB keys, and other random attacks are all part of such a threat landscape. In computer viruses, malicious code, including worms as well as run-time threats, can be utilized.
(d) Aggregate attack surface: Attacks can be launched from any layer that integrates people, networks, and systems.

3.2. Attack Vectors

(a) Storage of data in the cloud—Improper encryption, authentication, and access control of the cloud.
(b) Gateway connection to the cloud—Insufficient security mechanisms for device connectivity with the cloud.
(c) Storage of data in the gateway—Inadequate policy framework as well as a lack of strong encryption, verification, and authentication protocols at the entry point.
(d) Software/hardware/firmware vulnerabilities—Lack of proper guidelines for secure software development, insufficient update check firmware, and the application of malicious embedded hardware.
(e) Communication protocol—Appropriate security services are ineffective, as is the use of an old proprietary procedure and improper protocol setup.
(f) App connectivity—Lack of security control in app connectivity to the gateway by Wi-Fi.

3.3. Proposed Framework for Security Assessment

Early classification of medical equipment and health information is required to determine their significant risk threshold. An equipment disruption can put a patient's life in jeopardy; for instance, the equipment's privacy and security must be preserved to the highest possible level to prevent any starting point of disruption and also to decrease the potential threat to the bottom of the priority list. This study proposes a secure framework for evaluating the protection of medical equipment as well as health information. The proposed architecture is designed to evaluate the security of devices as well as the patient records produced by such secure devices. The IoMT security assessment framework is depicted in Figure 1.

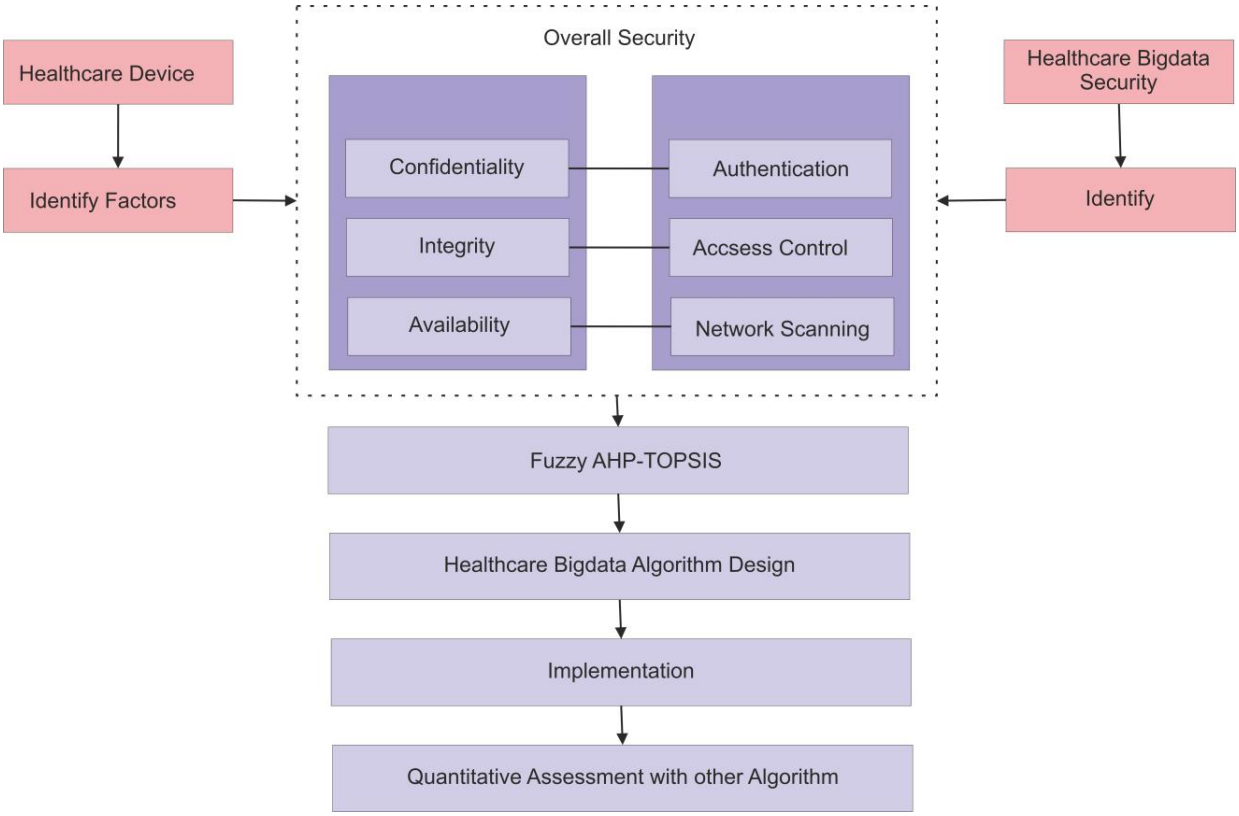


Figure 1. Framework to check the security of medical devices and healthcare big data.

(a) Device security checks to determine whether devices have security threats and weaknesses, as well as the strictest and most exact controls.
(b) Healthcare big data security checks and an applied security algorithm for securing the data.

Medical devices and data must go through security checks at an early stage in order to determine their major risk level. Device malfunctions will have an impact on the patient's life; therefore, device security and privacy must be maintained at the greatest level possible to stop any source of interruption and to reduce the risk of attack to the lowest level possible. Similarly, when data are generated by these devices and sent for processing (storing, cleaning, etc.) before being transferred to the doctor, during processing, attackers can modify the data; this modification of data can impact the patient's life.

As a result, devices and healthcare data will be subjected to risk assessment. Devices and data pose threats to humans, necessitating a variety of security management strategies to assure their protection and efficacy. A security evaluation is performed after identifying the security factors for both devices and data.

Security attributes are a collection of system inputs that can compromise a platform's security, and the same collection of security factors affects the security of the medical information recorded by such equipment. If the associated features are restricted as much as possible, the system could be more adaptable to being damaged. Attacks can come from persons, networks, systems, or any combination of the three and affect security measures such as authenticity, access control, and network scanning, which are related to confidentiality, integrity, and availability [36].

Security factors

(a) Confidentiality: For the privacy of healthcare data and related information, confidentiality is one of the most significant features of data protection elements. Service providers must ensure that data are not accessible to an unauthorized person.
(b) Integrity: Integrity is another important pillar of the data protection element, and it refers to data and information that will not be destroyed illegally.
(c) Availability: The third pillar of data protection is availability. Information should be accessible when it is needed on demand by an authorized authority from anywhere and at any time.

Further to the identification of security attributes, the appropriate safety control systems would be triggered and used to mitigate or completely eliminate damage. Security restrictions are carried out using the method of security factors. For instance, if information security factors are revealed, security mechanisms associated with network safeguards, such as network monitoring, digital certificates, and encryption, would then aid in handling the protection as well as obstructing attack techniques and tactics. System verification or authorization processes are used to restrict the reporting of processes and data supplies when the attacker is a system, and the security component is security and privacy. The system is also capable of detecting attacks. The underlying bases of trust as well as surveillance strategies are used to provide safeguards in this case.

As attackers attempt to modify data to gain access, ensuring security is a difficult endeavor. Using the suggested paradigm, researchers can gain a thorough understanding of medical device and healthcare data aspects, areas that can be penetrated for an assault, when and in what way the security is altered, and what this is worth in terms of danger. As a result, medical device and healthcare data security can be addressed early in the development process, before vulnerabilities are exploited. As a result, patients' data security will be improved.

As many authors have analyzed, this research demonstrates the essential categorization of all fundamentals, factors, and aspects that impact the security features of IoMT. The approach is hierarchical in structure and considers several security-related devices as alternatives. Because of its hierarchical system, as well as its tangible and intangible behavior, assessing IoMT security using the structure in Figure 2 may present challenges for multi-criteria decision making (MCDM).

3.4. Integrated Fuzzy AHP-TOPSIS Method

The goal of this study was to create an analytical security framework for the Internet of Medical Things for selecting the most appropriate tactic among several alternatives with the help of integrated AHP and TOPSIS techniques in a fuzzy setting. Fuzzy AHP has been used to calculate assessment preferential weights. Fuzzy TOPSIS is used to decrease the difference among performance improvement values as well as aspiration tiers and choose the appropriate process depending on numerous attributes of six alternative IoMT solutions.

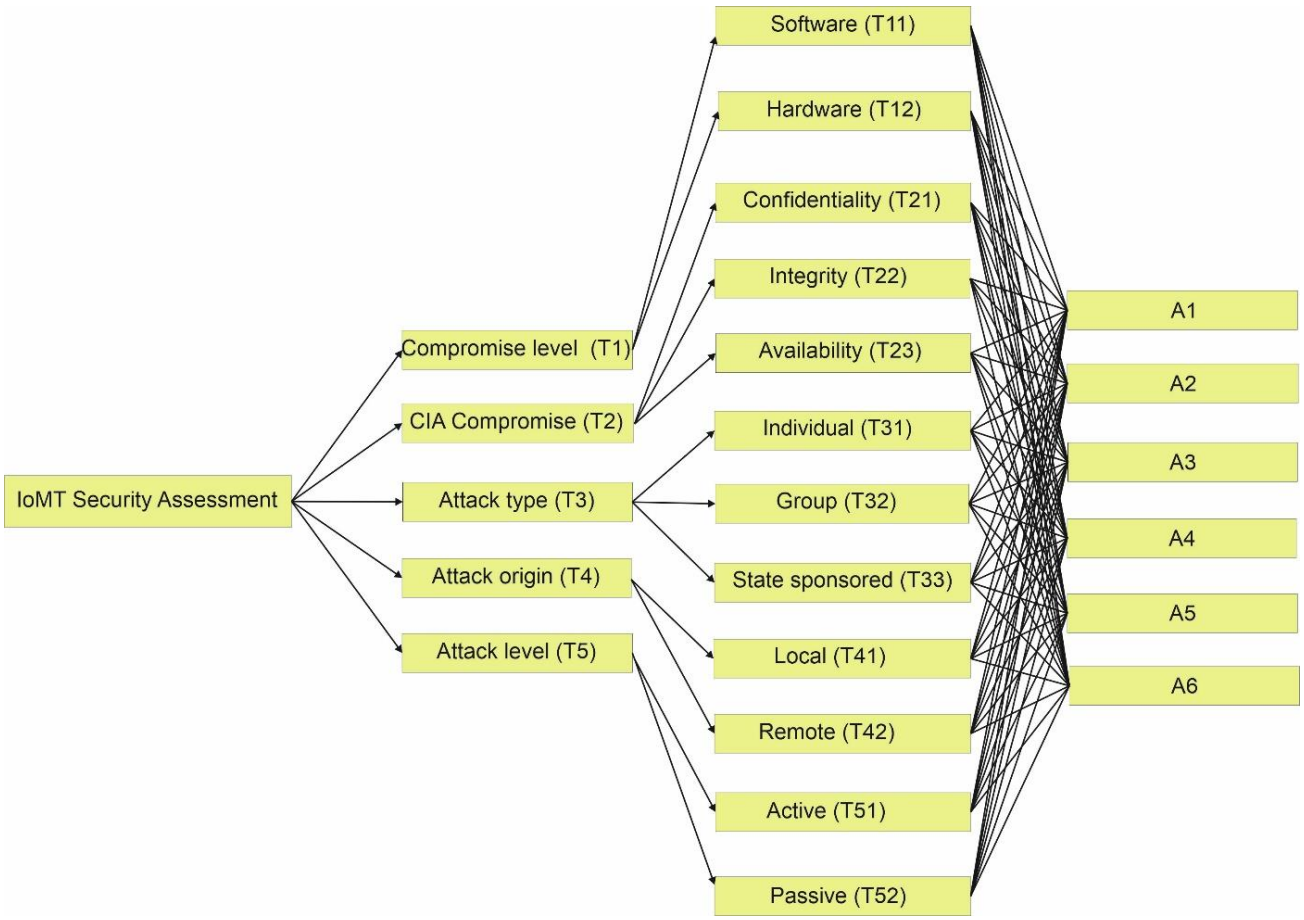


Figure 2. Hierarchy for the security evaluation of IoMT.

Fuzzy AHP: AHP is a procedure for assessing the significance of a range of processes in a problem in order to solve complicated decision-making problems [37–40]. The AHP method divides a multi-criteria selection challenge into a series of interconnected judgments. Moreover, the true AHP concept seems to have some flaws. The AHP technique is used well in most crisp-information judgment implementations; the AHP method generates and deals with a quite imbalanced scale of judgment [38,40]. The AHP technique ignores the ambiguity related to the process involved. To address these issues, numerous researchers have combined fuzzy set theory with AHP to reduce uncertainty. To ascertain the weights for summative components, fuzzy AHP is predicated on fuzzy timespan arithmetic with triangular fuzzy numbers (TFNs) as well as confidence indexes with an interval mean [41–43]. The assessment in this study is conducted with TFNs. The following are the stages in fuzzy AHP:

Step 1: Assessment hierarchy systems are constructed to identify the most suitable alternative among some of the given alternatives while taking into account the different criteria involved. The constructed hierarchy structure is used to choose the highest-quality alternative.

Step 2: Triangular fuzzy numbers are used to calculate the assessment component weights. This study employs TFNs for paired comparisons as well as computes fuzzy weights. The justification for employing a TFN is that it is simple to comprehend and measure for decision makers. Furthermore, modeling TFNs has been shown to be a successful method for articulating issues when the available information is subjective and

vague. The following describes the numerical technique for fuzzy AHP. A triplet (a1, a2, a3) can describe a triangular fuzzy number. The membership function $\mu\ \widetilde{A}\ (x)$ is defined by

$$\mu\ \widetilde{A}\ (x) = \begin{Bmatrix} \frac{x-l}{m-l}, & l \le x \le m, \\ \frac{u-x}{u-m}, & m \le x \le u, \\ 0, & otherwise. \end{Bmatrix} \quad (1)$$

Linguistic parameters take on the attributes characterized in their term set: they are a collection of linguistic aspects. Linguistic concepts are subjective classifications of linguistic parameters. A linguistic parameter is one with values that are phrases or sentences from a natural or artificial dialect. This type of interpretation is used here to compare and contrast two standards comparing assessment components utilizing nine basic linguistic phrases, namely, "Perfect", "Absolute", "Very good", "Fairly good", "Good", "Preferable", "Not Bad", "Weak advantage", and "Equal" on a fuzzy nine-tier scale. Every feature set (fuzzified scale) is characterized by three synchronous triangular fuzzy number variables: the left point as well as the middle point.

Step 3: Weights are chosen for multiple factors. The steps listed below are involved in determining weights for assessment criteria: (a) Decision makers input their judgment values to create a pair-wise comparative matrix that shows their preference for one criterion over another. Because the attributes are linguistic variables, they are represented by a triplet of triangular fuzzy figures. (b) The geometric mean technique is used to measure the synthesized pair-wise comparison matrix. r_i is characterized as the geometric mean.

$$r_i = \left(\mathrm{a}_{ij}^{1} \times \mathrm{a}_{ij}^{2} \ldots \mathrm{a}_{ij}^{10}\right)^{\frac{1}{10}} \quad (2)$$

Step 4: Every criterion's weight is assigned. This is accomplished by normalizing the matrix.

$$w_i = r_i \times (r_1 + r_2 + r_3 + \ldots + r_n)^1 \quad (3)$$

Step 5: For every weight, the Best Non-Fuzzy Performance (BNP) significance is decided. A weight's BNP value (l, m, u) is provided by the following equation.

$$\text{BNP value } = \frac{[(u-l)+(m-l)]}{3+l} \quad (4)$$

Step 6: Standards are consistently rated according to their BNP values. When comparing criteria, the standard with the higher BNP value is thought to have a bigger influence.

Fuzzy TOPSIS: The main idea behind the TOPSIS strategy is that the best suggested choice must not only be the closest to the positive ideal solution (PIS) but also be the furthest away from the negative ideal solution (NIS) [40–46]. TOPSIS has the benefit of requiring only restricted subjective input from decision makers as well as the strategy's ability to speedily determine the best alternate solution. The following are the stages involved in the fuzzy TOPSIS method.

Step 1: Standard weights are acquired from fuzzy AHP. The weight values of every characteristic under evaluation are included in the fuzzy AHP outcome.

Step 2: A fuzzy assessment matrix is produced. TFNs are used as transactions to summarize decision makers' judgments of attributes for every decision alternative that corresponds to each set of criteria.

Step 3: The fuzzy judgment matrix is standardized. The term R represents the normalized fuzzy decision matrix, and its elements are $[r_i]_{m\times n}; i = 1, 2, 3, \ldots, m$, where m is the complete number of criteria.

$$\widetilde{r}_{ij} = \left(\frac{l_{ij}}{u_j^+}, \frac{m_{ij}}{u_j^+}, \frac{u_{ij}}{u_j^+}\right) \quad (5)$$

where u_j^+ is the highest value in the whole fuzzy decision matrix.

Step 4: The points of reference for the fuzzy positive ideal as well as the fuzzy negative ideal are ascertained. The area compensation tactic defines fuzzy positive ideal solutions (FPIS) as well as fuzzy negative ideal solutions (FNIS).

$$\text{FPIS } A^{+} = \left(v_i^{+} \ldots v_j^{+} \ldots v_n^{+}\right) \tag{6}$$

$$\text{FNIS } A^{-} = \left(v_i^{-} \ldots v_j^{-} \ldots v_n^{-}\right) \tag{7}$$

where $v_i = (1,1,1) \times (w_j)$.

Step 5: The distance from FPIS (d^{+}) and the distance from FNIS (d^{-}) are recognized with the help of the following equations.

$$D_j^{+} = \sum_{j=1}^{n} d(\widetilde{v}_{ij}, \widetilde{v}_j^{*}) \; i = 1, 2, \ldots, m \tag{8}$$

$$D_j^{-} = \sum_{j=1}^{n} d(\widetilde{v}_{ij}, \widetilde{v}_j^{-}) \; i = 1, 2, \ldots, m \tag{9}$$

where d(a, b) is the range between two fuzzy figures, a and b. It is demarcated as

$$d\left(\widetilde{a}, \widetilde{b},\right) = \sqrt{\frac{1}{3}\left[(a_1 - b_1)^2 + (a_2 - b_2)^2 + (a_3 - b_3)^2\right]} \tag{10}$$

Step 6: The relative proximity to the ideal value is calculated, and the alternative solutions are ranked correspondingly. The relative proximity is provided through the following equation.

$$\widetilde{CC_i} = \frac{d_i^{-}}{d_i^{+} + d_i^{-}} \tag{11}$$

4. Results

This section provides a thorough interpretation and explanation of the quantitative findings. Healthcare device manufacturers are aiming for increased functionality while maintaining high security. Furthermore, serviceable security criteria impact plays a significant role in usable security throughout the design process of medical devices. As a result, the authors of this study present a fuzzy-based AHP-TOPSIS technique for determining the security of IoMT devices. The authors incorporated the categorized serviceable security characteristics mentioned in Section 3 of this article. Figure 2 depicts a hierarchical structure of serviceable security factors. For data collection, this research used the recommendations of 85 security professionals from both academia and industry via a survey questionnaire (which included questions about various characteristics of IoMT security). The researchers summarize the research outcomes in Tables 1–17 utilizing Equations (1)–(11). The following is an assessment of the serviceable security of IoMT devices using the proposed IoMT security assessment framework.

Table 1. Fuzzy pair-wise comparison matrix at level 1.

	T1	**T2**	**T3**	**T4**	**T5**
T1	1.000000, 1.000000, 1.000000	1.874000, 2.547000, 3.241000	1.476000, 1.678000, 1.957000	1.4864000, 2.454000, 3.386650	0.457000, 0.567000, 0.795000
T2	-	1.000000, 1.000000, 1.000000	0.615000, 0.785000, 1.036000	0.757100, 0.955000, 1.254000	0.165000, 0.250000, 0.25000
T3	-	-	1.000000, 1.000000, 1.000000	0.767000, 1.054000, 1.364000	0.214000, 0.257000, 0.310700

Table 1. *Cont.*

	T1	T2	T3	T4	T5
T4	-	-	-	1.000000, 1.000000, 1.000000	0.250000, 0.2354000, 0.290400
T5	-	-	-	-	1.000000, 1.000000, 1.000000

Table 2. Fuzzy aggregated pair-wise comparison matrix at level 2 for Compromise Level.

	T11	T12
T11	1.000000, 1.000000, 1.000000	0.304100, 0.397000, 0.561700
T12	-	1.000000, 1.000000, 1.000000

Table 3. Fuzzy aggregated pair-wise comparison matrix at level 2 for CIA Compromise.

	T21	T22	T23
T21	1.000000, 1.000000, 1.000000	0.417000, 0.558000, 0.795000	0.550000, 0.750000, 0.953000
T22	-	1.000000, 1.000000, 1.000000	0.795000, 0.885000, 1.023000
T23	-	-	1.000000, 1.000000, 1.000000

Table 4. Fuzzy aggregated pair-wise comparison matrix at level 2 for Attack Type.

	T31	T32	T33
T31	1.000000, 1.000000, 1.000000	0.551700, 0.585800, 0.664500	0.226600, 0.276400, 0.357300
T32	-	1.000000, 1.000000, 1.000000	0.693000, 0.882600, 1.125000
T33	-	-	1.000000, 1.000000, 1.000000

Table 5. Fuzzy aggregated pair-wise comparison matrix at level 2 for Attack Origin.

	T41	T42
T41	1.000000, 1.000000, 1.000000	0.569550, 0.784600, 1.154600
T42	-	1.000000, 1.000000, 1.000000

Table 6. Fuzzy aggregated pair-wise comparison matrix at level 2 for Attack Level.

	T51	T52
T51	1.000000, 1.000000, 1.000000	0.569870, 0.719510, 0.969950
T52	-	1.000000, 1.000000, 1.000000

Table 7. Defuzzified pair-wise comparison matrix.

	T1	T2	T3	T4	T5	Weights
T1	1.000000	2.554000	1.754000	2.434000	0.599400	0.240000
T2	0.392500	1.000000	0.796400	0.977700	0.245600	0.095000
T3	0.588100	1.251600	1.000000	1.056100	0.251300	0.122000
T4	0.411200	1.021400	0.941700	1.000000	0.231600	0.103000
T5	1.661900	4.812400	3.915000	4.241300	1.000000	0.442000
C.R. = 0.002515400						

Table 8. Aggregated pair-wise comparison matrix at level 2 for Compromise Level.

	T11	T12	Weights
T11	1.000000	0.414000	0.291000
T12	2.432450	1.000000	0.709000
C.R. = 0.000000			

Table 9. Aggregated pair-wise comparison matrix at level 2 for CIA Compromise.

	T21	T22	T23	Weights
T21	1.000000	0.571300	0.709100	0.242000
T22	1.744400	1.000000	0.895100	0.379000
T23	1.411100	1.118100	1.000000	0.380000
C.R. = 0.005800				

Table 10. Aggregated pair-wise comparison matrix at level 2 for Attack Type.

	T31	T32	T33	Weights
T31	1.000000	0.598100	0.284100	0.169000
T32	1.673100	1.000000	0.891100	0.349000
T33	3.512000	1.121300	1.000000	0.482000
C.R. = 0.022542500				

Table 11. Aggregated pair-wise comparison matrix at level 2 for Attack Origin.

	T41	T42	Weights
T41	1.000000	0.821400	0.452000
T42	1.211300	1.000000	0.548000
C.R. = 0.000000			

Table 12. Aggregated pair-wise comparison matrix at level 2 for Attack Level.

	T51	T52	Weights
T51	1.000000	0.741500	0.427000
T52	1.314300	1.000000	0.573000
C.R. = 0.000000			

Table 13. Overall weights and ranking of methods.

Main	Local Weights	Sub	Local Weights	Overall Weights
T1	0.240000	T11	0.291000	0.0698400
		T12	0.709000	0.1701600
T2	0.095000	T21	0.242000	0.0229900
		T22	0.379000	0.0360100
		T23	0.380000	0.0361000
T3	0.122000	T31	0.169000	0.0206200
		T32	0.349000	0.0425800
		T33	0.482000	0.0588100
T4	0.103000	T41	0.452000	0.0465600
		T42	0.548000	0.0564400
T5	0.442000	T51	0.427000	0.1887300
		T52	0.573000	0.2532700

Table 14. Subjective cognition results of evaluators in linguistic terms.

	A1	A2	A3	A4	A5	A6
T11	0.7300, 2.2700, 4.2700	2.8200, 4.8200, 6.7300	2.9100, 4.8200, 6.7300	0.7300, 2.2700, 4.2700	2.8200, 4.8200, 6.7300	2.8200, 4.8200, 6.7300
T12	4.4500, 6.4500, 8.1800	1.6400, 3.3600, 5.3600	0.7300, 2.2700, 4.2700	4.4500, 6.4500, 8.1800	0.7300, 2.2700, 4.2700	2.8200, 4.8200, 6.7300
T21	2.8200, 4.8200, 6.7300	0.7300, 2.2700, 4.2700	4.4500, 6.4500, 8.1800	0.7300, 2.2700, 4.2700	2.8200, 4.8200, 6.7300	1.6400, 3.3600, 5.3600
T22	0.7300, 2.2700, 4.2700	0.7300, 2.2700, 4.2700	0.7300, 2.2700, 4.2700	4.4500, 6.4500, 8.1800	1.6400, 3.3600, 5.3600	1.0000, 2.6400, 4.6400
T23	4.4500, 6.4500, 8.1800	4.4500, 6.4500, 8.1800	4.4500, 6.4500, 8.1800	2.8200, 4.8200, 6.7300	0.7300, 2.2700, 4.2700	2.8200, 4.8200, 6.7300
T31	0.7300, 2.2700, 4.2700	0.7300, 2.2700, 4.2700	0.7300, 2.2700, 4.2700	0.7300, 2.2700, 4.2700	0.7300, 2.2700, 4.2700	2.8200, 4.8200, 6.7300
T32	4.4500, 6.4500, 8.1800	4.4500, 6.4500, 8.1800	4.4500, 6.4500, 8.1800	4.4500, 6.4500, 8.1800	4.4500, 6.4500, 8.1800	1.6400, 3.3600, 5.3600
T33	2.8200, 4.8200, 6.7300	2.8200, 4.8200, 6.7300	2.8200, 4.8200, 6.7300	2.8200, 4.8200, 6.7300	0.7300, 2.2700, 4.2700	2.8200, 4.8200, 6.7300
T41	0.7300, 2.2700, 4.2700	0.7300, 2.2700, 4.2700	2.8200, 4.8200, 6.7300	0.7300, 2.2700, 4.2700	4.4500, 6.4500, 8.1800	1.6400, 3.3600, 5.3600
T42	4.4500, 6.4500, 8.1800	4.4500, 6.4500, 8.1800	1.6400, 3.3600, 5.3600	4.4500, 6.4500, 8.1800	2.8200, 4.8200, 6.7300	1.0000, 2.6400, 4.6400

Table 14. *Cont.*

	A1	A2	A3	A4	A5	A6
T51	2.8200, 4.8200, 6.7300	2.8200, 4.8200, 6.7300	1.0000, 2.6400, 4.6400	2.8200, 4.8200, 6.7300	1.6400, 3.3600, 5.3600	0.7300, 2.2700, 4.2700
T52	1.6400, 3.3600, 5.3600	1.6400, 3.3600, 5.3600	0.7300, 2.2700, 4.2700	1.6400, 3.3600, 5.3600	2.8200, 4.8200, 6.7300	1.0000, 2.6400, 4.6400

Table 15. The normalized fuzzy decision matrix.

	A1	A2	A3	A4	A5	A6
T11	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800	0.5200, 0.7400, 0.9200
T12	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800	0.4600, 0.6700, 0.8600
T21	0.3800, 0.6000, 0.8000	0.4600, 0.6700, 0.8600	0.3800, 0.6000, 0.8000	0.3800, 0.6000, 0.8000	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800
T22	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800	0.4600, 0.6700, 0.8600	0.5400, 0.7500, 0.9200
T23	0.4600, 0.6700, 0.8600	0.3800, 0.6000, 0.8000	0.3800, 0.6000, 0.8000	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800	0.4600, 0.6700, 0.8600
T31	0.6100, 0.8200, 0.9800	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800
T32	0.6100, 0.8200, 0.9800	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.3800, 0.6000, 0.8000	0.3800, 0.6000, 0.8000	0.4600, 0.6700, 0.8600
T33	0.3800, 0.6000, 0.8000	0.3800, 0.6000, 0.8000	0.6100, 0.8200, 0.9800	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800	0.5200, 0.7400, 0.9200
T41	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800	0.4600, 0.6700, 0.8600
T42	0.6000, 0.8100, 1.0000	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800	0.4600, 0.6700, 0.8600
T51	0.5200, 0.7400, 0.9400	0.4600, 0.6700, 0.8600	0.3800, 0.6000, 0.8000	0.3800, 0.6000, 0.8000	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800
T52	0.4200, 0.6900, 0.9900	0.6100, 0.8200, 0.9800	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800	0.5200, 0.7400, 0.9200	0.5400, 0.7500, 0.9200

Table 16. The weighted normalized fuzzy decision matrix.

	A1	A2	A3	A4	A5	A6
T11	0.0020, 0.0100, 0.0390	0.0020, 0.0080, 0.0250	0.0020, 0.0080, 0.0250	0.0020, 0.0100, 0.0390	0.0020, 0.0100, 0.0390	0.0020, 0.0060, 0.0200
T12	0.0020, 0.0080, 0.0250	0.0020, 0.0080, 0.0250	0.0020, 0.0070, 0.0220	0.0010, 0.0040, 0.0170	0.0010, 0.0040, 0.0170	0.0030, 0.0120, 0.0420
T21	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0220	0.0030, 0.0120, 0.0420	0.0020, 0.0080, 0.0250	0.0020, 0.0080, 0.0250	0.0020, 0.0070, 0.0220
T22	0.0030, 0.0120, 0.0420	0.0030, 0.0120, 0.0420	0.0020, 0.0080, 0.0250	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0220	0.0030, 0.0120, 0.0420
T23	0.0030, 0.0120, 0.0420	0.0020, 0.0080, 0.0250	0.0020, 0.0080, 0.0250	0.0030, 0.0120, 0.0420	0.0030, 0.0120, 0.0420	0.0020, 0.0080, 0.0250
T31	0.0020, 0.0070, 0.0220	0.0030, 0.0120, 0.0420	0.0020, 0.0070, 0.0220	0.0030, 0.0120, 0.0420	0.0020, 0.0080, 0.0250	0.0020, 0.0080, 0.0250
T32	0.0020, 0.0080, 0.0250	0.0020, 0.0080, 0.0250	0.0020, 0.0080, 0.0250	0.0020, 0.0080, 0.0250	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0220
T33	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0220	0.0030, 0.0120, 0.0420	0.0030, 0.0120, 0.0420
T41	0.0030, 0.0120, 0.0420	0.0030, 0.0120, 0.0420	0.0030, 0.0120, 0.0420	0.0030, 0.0120, 0.0420	0.0030, 0.0120, 0.0420	0.0020, 0.0080, 0.0250
T42	0.0030, 0.0120, 0.0420	0.0020, 0.0080, 0.0250	0.0030, 0.0120, 0.0420	0.0020, 0.0080, 0.0250	0.0020, 0.0100, 0.0390	0.0030, 0.0120 0.0420
T51	0.0020, 0.0070, 0.0250	0.0030, 0.0120, 0.0420	0.0010, 0.0050, 0.0180	0.0000, 0.0040, 0.0170	0.0300, 0.0120, 0.0420	0.0020, 0.0080, 0.0250
T52	0.0010, 0.0050, 0.0180	0.0020, 0.0080, 0.0250	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0240	0.0020, 0.0080, 0.0250	0.0010, 0.0050, 0.0180

Table 17. Satisfaction degree for the aspired level among different alternatives.

Alternatives	dist+i	dist-i	Gap Degree of CC+i	Satisfaction Degree of CC-i
A1	0.0515245	0.038569	0.3655859	0.62585971
A2	0.0655254	0.037589	0.5248597	0.64446598
A3	0.0475698	0.058564	0.5698569	0.44458799
A4	0.0457584	0.038697	0.2562567	0.52112533
A5	0.4518574	0.055988	0.5656599	0.46689221
A6	0.0452859	0.055857	0.6125874	0.38888923

Pair-wise comparison matrices of level 1 characteristics are determined by calculations during the MCDM process and are presented in Table 1. Further, fuzzy aggregated pair-wise comparison matrices at level 2 for the Compromise Level, CIA Compromise, Attack

Type, Attack Origin, and Attack Level are presented in Table 2, Table 3, Table 4, Table 5, and Table 6, respectively. After creating the pair-wise comparison, defuzzification is used to generate a measurable value depending on the determined TFN scores. Table 7 shows the defuzzified pair-wise comparison matrix. Further aggregated pair-wise comparison matrices at level 2 for the Compromise Level, CIA Compromise, Attack Type, Attack Origin, and Attack Level are presented in Tables 8–12, respectively. Table 13 shows the overall weights and ranking of methods. Further, TFNs were calculated by converting etymological aspects into numeric indicators. The tables contain the evaluation measurements as well as the TFN aspects. Table 14 shows the subjective cognition results of evaluators in linguistic terms. Table 15 presents the normalized fuzzy decision matrix. Table 16 shows the weighted normalized fuzzy decision matrix. Finally, Table 17 and Figure 3 show the Satisfaction Degree for the aspired level among the different alternatives. Table 17 shows how the scores of dist+i and dist-i, followed by Gap Degree and Satisfaction Degree values, were estimated to prioritize the various alternatives. To weight the different alternative solutions, Satisfaction Degree figures were taken into account.

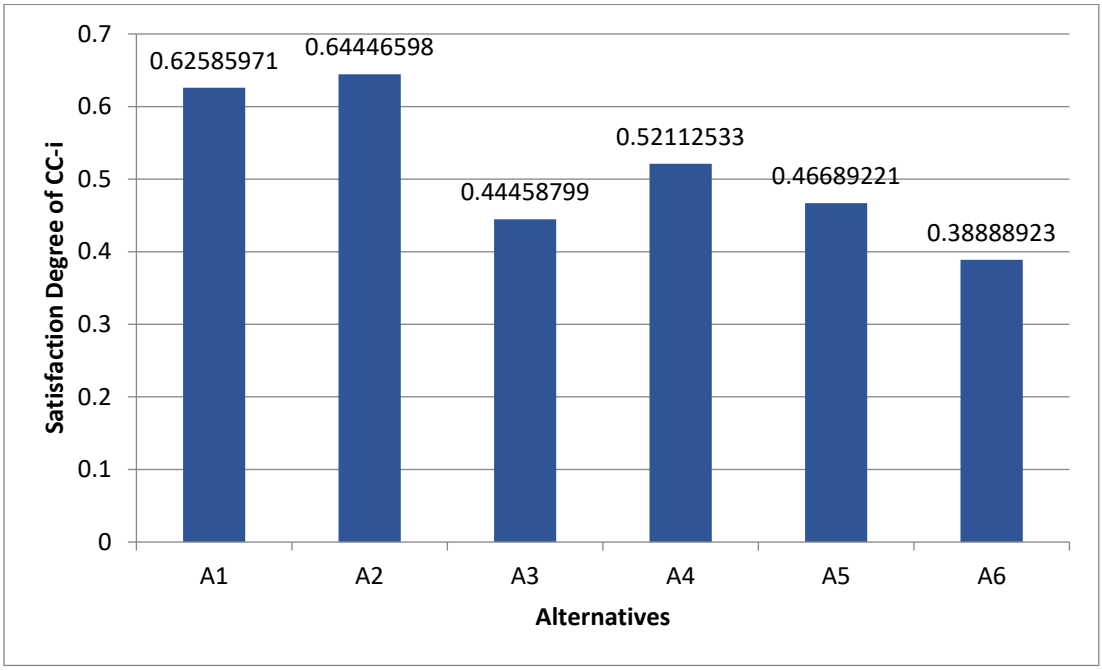


Figure 3. Satisfaction Degree of CC-i.

The security assessment of IoMT is presented in this study. A diagrammatic illustration of the research results from this study is shown in Figure 3. The results show that satisfaction levels for A1, A2, A3, A4, A5, and A6 are estimated to be 0.62585971, 0.64446598, 0.44458799, 0.52112533, 0.46689221, and 0.38888923, respectively. The findings demonstrate that A2 has the highest security priority when it comes to the selection of effective and highly secure IoMT devices.

5. Discussion

With the introduction of interconnected medical devices, cutting-edge technological innovations have altered the complexities of healthcare organizations. As a consequence, there has been a surge in involvement in medical device information security. Furthermore, it has been determined that the adoption of new communication technologies, including 5G networks, will completely transform the healthcare market. IoT security is complicated, and it is evident that conventional cybersecurity measures are no longer adequate. Comprehending and minimizing the effects on the thousands of connected devices discovered in the network require device recognition as well as firmware analysis. Viewing only a portion

of the scenario puts healthcare organizations, as well as the communities they represent, in more jeopardy now than ever before. The IoMT platform's utmost goal is to collect and communicate health information such as ECGs, weight, pulse rate, insulin levels, etc. Such information may be disclosed to an authorized person, who could be a doctor, an involved health organization, an insurance company, or perhaps an external consultant, irrespective of time, place, or tool. However, the tale is not as straightforward since IoMT is vulnerable to a variety of evolving cyberattacks. Since an attacker exploits the fact that this industry is worth billions of dollars, new ransomware attacks are developed and initiated on IoMT devices every day. The main objective of this study was to design and develop a security assessment framework for IoMT devices.

The security assessment of different IoMT devices is presented in this research study. The intensity and difficulty of characterizing security profile information is a significant challenge for the suggested framework. This seems to be due to the extensive pool of evaluation characteristics provided by the framework. The researchers hope that this work inspires technology solution providers to collaborate in order to compete straightforwardly as well as meet the needs of clients. Furthermore, the evaluation attributes may be difficult to comprehend, particularly for inexperienced users, including patients and healthcare workers, who frequently lack software and operational understanding. We are confident that this work will motivate them to understand possible security concerns as well as mitigation strategies. We predict that the proposed framework will be utilized only when incorporating, improving, or designing IoMT services. As a result, we strongly recommend IoMT participants to engage their time as well as dedication in the process because it will then enable them to explore and avoid serious security implications.

6. Conclusions and Future Work

Medical devices are unsecure in the design and post-market phases and may be vulnerable to cyber threats as the quantity and complexity of cyber threats grow. Similarly, the healthcare data generated by these devices are also unsecure. If their vulnerabilities are not addressed and remedied, these dangers can be leveraged as an entry point into a hospital. Cyber threats have a huge attack surface, which might disrupt healthcare and possibly put patients' lives in jeopardy. Because healthcare data generated by the devices are sent to the cloud for processing, any modification to the data during processing may threaten the lives of patients. With the growing number of connected medical devices, the probability of being exposed to attack surfaces and vulnerabilities by malevolent attackers is increasing. It is important to counter cyberattacks by including security methods to reduce attacks. This study proposes a security assessment of different medical devices in the design and post-market phases and data security assessment. This research investigates a conceptual model that incorporates increased security principles into the design and implementation of medical instruments as well as data protection during handling. This framework is used for medical devices and healthcare data security assessment and develops the security algorithm for data security. To evaluate the security of devices and data, the authors applied an integrated fuzzy AHP TOPSIS approach in the proposed model. This methodology is useful for the assessment of cyber threats to devices and data and the development of a security algorithm for securing healthcare data.

The suggested framework can safely and securely enhance medical device interoperability and healthcare data security in healthcare, which is essential to protect patients' healthcare data privacy. The framework has the ability to check different healthcare devices' security, as well as the efficiency of the security mechanisms used in mitigating or blocking attacks. Regardless of the fact that our research study makes use of the potential of integrated fuzzy AHP TOPSIS, numerous methods for identifying and prioritizing security performance measures for IoMT devices could be incorporated with fuzzy logic. As a result, in future work, numerous different MCDM tactics, such as ANP, ELECTRA, VIKOR, PROMETHEUS, and so on, may be employed for comparative evaluation.

Author Contributions: Conceptualization, F.A.A. and M.T.J.A.; Data curation, F.A.A., M.A. and M.T.J.A.; Formal analysis, F.A.A., M.A. and M.T.J.A.; Funding acquisition, F.A.A.; Investigation, F.A.A. and M.T.J.A.; Methodology, F.A.A. and M.T.J.A.; Project administration, F.A.A. and M.T.J.A.; Resources, M.A. and M.T.J.A.; Software, F.A.A., M.A. and M.T.J.A.; Supervision, F.A.A. and M.T.J.A.; Validation, M.A. and M.T.J.A.; Visualization, M.A. and M.T.J.A.; Writing—original draft, F.A.A., M.A. and M.T.J.A.; Writing—review & editing, F.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: The work is funded by grant number 12-INF2970-10 from the National Science, Technology and Innovation Plan (MAARIFAH), the King Abdul-Aziz City for Science and Technology (KACST), Kingdom of Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We thank the Science and Technology Unit at Umm Al-Qura University for their continued logistics support.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rahman, A.; Asyhari, A.T. The Emergence of Internet of Things (IoT): Connecting Anything, Anywhere. *Computers* **2019**, *8*, 40. [CrossRef]
2. Ahmad, M.; Al-Amri, J.F.; Subahi, A.F.; Khatri, S.; Seh, A.H.; Nadeem, M.; Agrawal, A. Healthcare device security assessment through computational methodology. *Comput. Syst. Sci. Eng.* **2021**, *41*, 811–828. [CrossRef]
3. Uzialko, A. Connected Medical Device Security. Available online: https://www.businessnewsdaily.com/15031-connected-medical-devices-healthcare-cybersecurity.html. (accessed on 11 July 2022).
4. Alhakami, W.; Baz, A.; Alhakami, H.; Ahmad, M.; Khan, R.A. Healthcare device security: Insights and implications. *Intell. Autom. Soft Comput.* **2021**, *27*, 409–424. [CrossRef]
5. Rushanan, M.; Rubin, A.D.; Kune, D.F.; Swanson, C.M. SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014; IEEE: New York, NY, USA; pp. 524–539. [CrossRef]
6. Algarni, A.; King Abdulaziz University; Ahmad, M.; Attaallah, A.; Agrawal, A.; Kumar, R.; Khan, R. A hybrid fuzzy rule-based multi-criteria framework for security assessment of medical device software. *Int. J. Intell. Eng. Syst.* **2020**, *13*, 51–62. [CrossRef]
7. Vaas, L. Doctors Disables Wireless in Dick Cheney's Pacemaker to Thwart Hacking. *Nakedsecurity Sophis*. 22 October 2013. Available online: https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/ (accessed on 11 July 2022).
8. Vora, K.; Schaeffer, M. A platform approach to securing your medical devices. White paper. *Renesas Electron.* **2017**, *5*.
9. Rabinowitz, J. Protecting Patients with Cybersecurity. Healthcare GLOBAL. 2018. Available online: https://www.healthcareglobal.com/technology/protecting-patients-cybersecurity (accessed on 11 July 2022).
10. Rondon, L.P.; Babun, L.; Aris, A.; Akkaya, K.; Uluagac, A.S. Survey on enterprise Internet-of-Things systems (E-IoT): A security perspective. *Ad Hoc Netw.* **2022**, *125*, 102728. [CrossRef]
11. Yaqoob, T.; Abbas, H.; Atiquzzaman, M. Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3723–3768. [CrossRef]
12. Hanna, S.; Rolles, R.; Molina-Markham, A.; Poosankam, P.; Blocki, J.; Fu, K.; Song, D. Take two software updates and see me in the morning: The case for software security evaluations of medical devices. In Proceedings of the 2nd USENIX Workshop on Health Security and Privacy, San Francisco, CA, USA, 8–12 August 2011.
13. Dey, N.; Ashour, A.S.; Shi, F.; Fong, S.J.; Tavares, J.M.R. Medical cyber-physical systems: A survey. *J. Med. Syst.* **2018**, *42*, 1–13. [CrossRef]
14. Savage, T. The implications of RoHS on active implantable medical devices. In Proceedings of the 2011 International Reliability Physics Symposium, Monterey, CA, USA, 10–14 April 2011.
15. Chen, M.; Gonzalez, S.; Vasilakos, A.; Cao, H.; Leung, V. Body Area Networks: A Survey. *Mob. Netw. Appl.* **2010**, *16*, 171–193. [CrossRef]
16. Ankaralı, Z.E.; Abbasi, Q.H.; Demir, A.F.; Serpedin, E.; Qaraqe, K.; Arslan, H. A comparative review on the security research for wireless implantable medical devices. In Proceedings of the International Conference on Wireless Mobile Communication and Healthcare, Athens, Greece, 3–5 November 2014.
17. Lee, I.; Sokolsky, O.; Chen, S.; Hatcliff, J.; Jee, E.; Kim, B.; King, A.; Mullen-Fortino, M.; Park, S.; Roederer, A.; et al. Challenges and research directions in medical cyber–physical systems. *Proc. IEEE* **2012**, *100*, 75–90.

18. Haque, S.; Aziz, S.; Rahman, M. Review of Cyber-Physical System in Healthcare. *Int. J. Distrib. Sens. Netw.* **2014**, *2014*, 217415. [CrossRef]
19. Rostami, M.; Burleson, W.; Juels, A.; Koushanfar, F. Balancing security and utility in medical devices? In Proceedings of the 50th ACM/EDAC/IEEE Design Automation Conference (DAC), Austin, TX, USA, 29 May–7 June 2013.
20. Kavianpour, S.; Shanmugam, B.; Zolait, A.; Razaq, A. A Framework to Detect Cyber-attacks against Networked Medical Devices (Internet of Medical Things): An Attack-Surface-Reduction by Design Approach. *Int. J. Comput. Digit. Syst.* **2021**, *11*, 1–12.
21. Halperin, D.; Heydt-Benjamin, T.; Ransford, B.; Clark, S.; Defend, B.; Morgan, W.; Fu, K.; Kohno, T.; Maisel, W. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In Proceedings of the IEEE Symposium on Security and Privacy (sp 2008), Oakland, CA, USA, 18–22 May 2008.
22. Gollakota, S.; Hassanieh, H.; Ransford, B.; Katabi, D.; Fu, K. They can hear your heartbeats: Noninvasive security for implantable medical devices. In Proceedings of the ACM SIGCOMM 2011 conference (SIGCOMM '11), Toronto, ON, Canada, 15–19 August 2011.
23. Chen, G.; Rodriguez-Villegas, E. System-level design trade-offs for truly wearable wireless medical devices. In Proceedings of the Annual International Conference of the IEEE on Engineering in Medicine and Biology Society (EMBC), Buenos Aires, Argentina, 31 August–4 September 2010.
24. Mitchell, R.; Chen, I.R. Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems. *IEEE Trans. Dependable Secur. Comput.* **2014**, *12*, 16–30. [CrossRef]
25. Xu, F.; Qin, Z.; Tan, C.; Wang, B.; Li, Q. IMDGuard: Securing implantable medical devices with the external wearable guardian. In Proceedings of the IEEE International Conference on Computer Communications (INFOCOM 2011), Shanghai, China, 10–15 April 2011.
26. Hayajneh, T.; Mohd, B.J.; Imran, M.; Almashaqbeh, G.; Vasilakos, A.V. Secure authentication for remote patient monitoring with wireless medical sensor networks. *Sensors* **2016**, *16*, 424. [CrossRef]
27. Guo, L.; Zhang, C.; Sun, J.; Fang, Y. PAAS: A privacy-preserving attribute-based authentication system for eHealth networks. In Proceedings of the 32nd International Conference on Distributed Computing Systems, Macau, China, 18–21 June 2012; IEEE: New York, NY, USA, 2012.
28. Li, C.-T.; Lee, C.-C.; Weng, C.-Y. A secure cloudassisted wireless body area network in mobile emergency medical care system. *J. Med. Syst.* **2016**, *40*, 117. [CrossRef]
29. Lounis, A.; Hadjidj, A.; Bouabdallah, A.; Challal, Y. Healing on the cloud: Secure cloud architecture for medical wireless sensor networks. *Future Gener. Comput. Syst.* **2016**, *55*, 266–277. [CrossRef]
30. Gao, S.; Thamilarasu, G. Machine-learning classifiers for security in connected medical devices. In Proceedings of the 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada, 31 July–3 August 2017; IEEE: New York, NY, USA, 2017.
31. Liu, F.; Li, T. A clustering k-anonymity privacypreserving method for wearable IoT devices. *Secur. Commun. Netw.* **2018**, *2018*, 4945152. [CrossRef]
32. Humayed, A.; Lin, J.; Li, F.; Luo, B. Cyberphysical systems security—A survey. *IEEE Internet Things J.* **2017**, *4*, 1802–1831. [CrossRef]
33. Sun, J.; Yao, X.; Wang, S.; Wu, Y. Blockchain-based secure storage and access scheme for electronic medical records in IPFS. *IEEE Access* **2020**, *8*, 59389–59401. [CrossRef]
34. Ari, J.; Ristenpart, T. Honey encryption beyond the brute-force barrier. *IEEE Comput. Reliab. Soc.* **2014**, *78*, 587–601.
35. Kapil, G.; Agrawal, A.; Khan, R.A. Attribute based honey encryption algorithm for securing big data: Hadoop distributed file system perspective. *PeerJ Comput. Sci.* **2020**, *6*, e259. [CrossRef] [PubMed]
36. Yang, C.; In, W.L.; Liu, M. A novel triple encryption scheme for Hadoop-based cloud data security. *Emerg. Intell. Data Web Technol.* **2013**, *2*, 437–442.
37. Al-Zahrani, F.A. Subscription-based data-sharing model using blockchain and data as a service. *IEEE Access* **2020**, *8*, 115966–115981. [CrossRef]
38. Naz, M.; Al-zahrani, F.A.; Khalid, R.; Javaid, N.; Qamar, A.M.; Afzal, M.K.; Shafiq, M. A secure data sharing platform using blockchain and interplanetary file system. *Sustainability* **2019**, *11*, 7054. [CrossRef]
39. Al-Zahrani, F.A. Evaluating the usable-security of healthcare software through unified technique of fuzzy logic, ANP and TOPSIS. *IEEE Access* **2020**, *8*, 109905–109916. [CrossRef]
40. Ansari, M.T.; Agrawal, A.; Khan, R.A. DURASec: Durable Security Blueprints for Web-Applications Empowering Digital India Initiative. *EAI Endorsed Trans. Scalable Inf. Syst.* **2022**, e25. [CrossRef]
41. Shahid, A.; Almogren, A.; Javaid, N.; Al-Zahrani, F.A.; Zuair, M.; Alam, M. Blockchain-based agri-food supply chain: A complete solution. *IEEE Access* **2020**, *8*, 69230–69243. [CrossRef]
42. Ansari MT, J.; Al-Zahrani, F.A.; Pandey, D.; Agrawal, A. A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development. *BMC Med. Inform. Decis. Mak.* **2020**, *20*, 236. [CrossRef]
43. Seh, A.H.; Al-Amri, J.F.; Subahi, A.F.; Ansari MT, J.; Kumar, R.; Bokhari, M.U.; Khan, R.A. Hybrid computational modeling for web application security assessment. *CMC-Comput. Mater. Contin.* **2022**, *70*, 469–489.

44. Alosaimi, W.; Ansari, M.T.J.; Alharbi, A.; Alyami, H.; Ali, S.; Agrawal, A.; Khan, R.A. Toward a unified model approach for evaluating different electric vehicles. *Energies* **2021**, *14*, 6120. [CrossRef]
45. Alyami, H.; Nadeem, M.; Alharbi, A.; Alosaimi, W.; Ansari, T.J.; Pandey, D.; Kumar, R.; Khan, R.A. The Evaluation of Software Security through Quantum Computing Techniques: A Durability Perspective. *Appl. Sci.* **2021**, *11*, 1784. [CrossRef]
46. Alyami, H.; Ansari, T.J.; Alharbi, A.; Alosaimi, W.; Alshammari, M.; Pandey, D.; Agrawal, A.; Kumar, R.; Khan, R.A. Effectiveness Evaluation of Different IDSs Using Integrated Fuzzy MCDM Model. *Electronics* **2022**, *11*, 859. [CrossRef]