I. J. Education and Management Engineering, **2024, 2, 41-52**
Published Online on April 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijeme.2024.02.04

Determination of Security Factors Affecting Internet of Medical Things by Artificial Intelligence Technique

Mohd. Nadeem*
School of Computer Application, Babu Banarasi Das University, Lucknow, India
Email: mohd.nadeem1155@gmail.com
ORCID iD: https://orcid.org/ 0000-0003-4244-8076
*Corresponding Author

Prabhash Chandra Pathak
School of Computer Application, Babu Banarasi Das University, Lucknow, India
Email: pathakprabhash2@gmail.com
ORCID iD: https://orcid.org/ 0000-0001-5704-0028

Mahfooz Ahmad
Department of Computer Application, Integral University, Lucknow, India
Email: ahmadmahfooz1@gmail.com
ORCID iD: https://orcid.org/ 0009-0004-1119-9710

Masood Ahmad
Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, India
Email: ermasood@gmail.com
ORCID iD: https://orcid.org/ 0000-0002-7859-8327

Received: 01 August, 2023; Revised: 12 October, 2023; Accepted: 03 December, 2023; Published: 08 April, 2024

Abstract: In the age of computing, there is a vast assortment of medical equipment and software available. Software and medical equipment that can be online connected to healthcare Information Technology (IT) systems are referred to as Internet of Medical Things (IoMT). This research study elaborates healthcare connectivity and its security issues to the different dimension of IoMT. During the pandemic situation in 2020-21 Covid, importance of virtualization and its dependencies have got the momentum. The security challenge of IoMT needs to be addressed. The research analysis is evaluating the impact of security factors in IoMT. By systematically evaluating research studies based on the keywords IoMT, security of IoMT, and security in healthcare sector, security attributes and factors were discovered from the different digital library. This evaluation uses soft computing and Artificial Intelligence (AI) techniques, quantitatively elaborates the factors of IoMT and their impact based on security. The results provide guidance for the development of IoMT with security attributes that can help to ensure the security of the device and software based applications on networks or in the cloud. To assess the importance of the criteria and the ranking of the alternatives, the AI technique of Analytic Hierarchy Process (AHP) and Technique for Order of Preferences by Similarity to Ideal Solution (TOPSIS) were applied. The hybrid Fuzzy AHP, Fuzzy TOPSIS techniques are utilizing the concept of decision making in security of IoMT. The items were evaluated using a multi rules choice investigation with several standards. In this research study, eight factors and ten alternatives of IoMT were selected to determine their impact on security. The creating new funding, operating and business model factor of IoMT got the top weight and successfully navigating regulatory change got the least. The AI research on IoMT security determination helps the developer, medical practitioner, and medical device operator to consider the impact of security in IoMT.

Index Terms: IoMT, IoT, Fuzzy AHP, AI, Healthcare Security, Fuzzy TOPSIS.

1. Introduction

The Wi-Fi enabled medical devices are connecting to cloud infrastructure like amazon web services. This makes machine to machine communication possible in IoMT. The IoMT allows remote patient monitoring for people with chronic diseases. Patient wearable devices communicate with prescribers or doctors. IoMT keeps track of hospital admissions and prescription orders. IoMT technology can also be used to convert or monitor medical equipment, such as infusion pumps and hospital beds with sensors with the integration of near field communication radio frequency identification tags in consumer mobile devices. There are now more potential applications for the IoMT, similar to the larger IoT problem. Medical supplies and equipment can have tags to track stock levels. The IoMT enables telemedicine for remote patient monitoring from home. Medical care providers are worried about the security of sensitive information. The Health Insurance Portability and Accountability Act (HIPAA) protect health data is transmitted via IoMT. Security of sensitive data is a growing concern in IoMT [1]. The medical technology sector produces around 500,000 distinct types of medical equipment. These include of implanted gadgets like pacemakers and defibrillators, portable gadgets like skin patches and insulin pumps, and stationary gadgets like home monitoring and scanning equipment. These tools and devices are widely used in interactions between patients and the healthcare system. IoT technologies are having a revolutionary effect on the healthcare industry, as they do on many other industries, since innovation in the creation of connected medical devices is being driven by developments in wireless technology, miniaturization, computation, and processing power. The growth of connected medical devices and improvements in connection services, software, and systems gave rise to the IoMT. Improved connection might be advantageous for most medical devices. This has made it possible to gather and transmit high quality medical data.

In order to track and alter patient behavior and health state in real time during hasten diagnosis treatment will improve the accuracy. The IoMT bridges the gap between the digital and physical worlds by streamlining clinical processes, data, and workflows, improving operational efficiency and productivity in healthcare sector. By connecting patients, carers, doctors, patient or performance data, care delivery, and patient support, linked medical devices and mobile applications greatly improve patient outcomes. Although IoT has the potential to address issues with healthcare costs, accessibility, and care coordination, gathering data from millions of linked medical devices won't be beneficial until it is converted into information. The future awakens phrase make six forecasts, and each one largely relies on connected medical technology. The development and success of the medical services, life sciences, and industries are anticipated in 2022 as a result of the developments and implementation of linked clinical devices. The IoMT market was valued at $41.2 billion as of 2017 and is anticipated to grow to $158.1 billion by 2022, according to markets and markets magazine article. By 2022, it is anticipated that the market for connected clinical devices, which include tools for patient assessment, evaluation, and treatment, would grow significantly. The spread of IoMT and rising healthcare expenses are related. Global health care spending is anticipated to increase by 4.2% yearly from $7.1 trillion in 2015 to $8.7 trillion by 2020, in part because of an ageing population. As a result, unless significant reforms are implemented, health care's risks becoming extremely pricey in many countries.

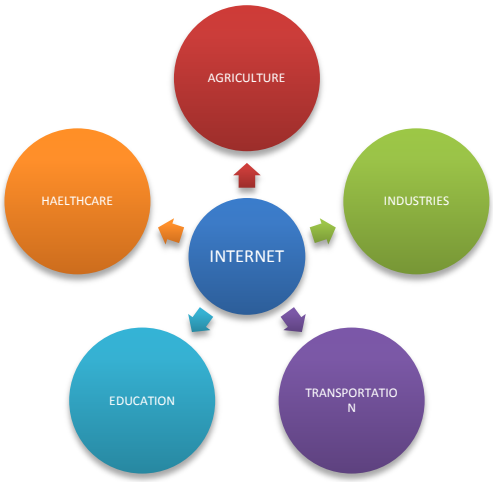

Fig. 1. The role of IoT in different domain

The medical technology industry can support the transition to value based care, enhance care quality and efficiency, and reduce costs. However, the industry needs to address systemic issues and opportunities to benefit fully from the IoMT. The IoT is a framework that connects computers, devices, people, animals, and objects with unique IDs that may afterwards exchange information. Transportation, healthcare, industrial automation, and energy are some areas that the IoT may improve. Smart houses are made feasible by the system, which comprises thermostat monitoring and control systems for heating, ventilation, and air conditioning. Figure 1 illustrates the different uses of the Internet of Things.

The quantitative analysis of IoMT further divided by section related work; we explain research development in different aspects of IoMT. Further different factors are identified by the experts and alternatives of IoMT are explained and its connectivity represented by the hierarchy diagram. In this section, the Neural Network F-AHP is explained as AI method used to evaluate factors. The following section describes the research findings, and the conclusion is presented last.

2. Literature Review

The [2] are suggesting an IoT based system for monitoring data congestion that has a distinct area of structure and relies on cutting edge technology to encourage traffic control. [3] The IoT may be used to track environmental conditions using crisis alarms, sullying control, and disappointment indicators. The IoT applications in healthcare present the greatest research challenges given the existing environment. With the current pandemic, it is risky to go to a doctor for minor issues. As a result, we are able to independently take preventative measures because IoMT devices make it simple for us to keep an eye on our daily health data.

The researcher [4] identifying network intrusions, mediating security attacks against IoMT systems [5]. To assure security in the IoT, IoMT devices are used for web based security review, and AI can be utilised to automatically inform necessary parties in the case of an emergency. The AI based devices are utilised to give medical care and track patient information. Furthermore, IoMT network can be secured with blockchain technology by digitally storing confidential and decentralised data without the need for a third party. This can be used by medical servers that include electronic health records, such as medical record, to restrict rights and access to medical data [6]. In order to avoid being sent to hospitals, nursing homes, or other incarceration facilities, people receiving homecare can now live more easily and sustain a healthy lifestyle thanks to smart home technologies. For older or disabled people, this is especially crucial. The IoMT will improve healthcare services for patients, staff, and doctors, reducing feelings of stress, despair, and isolation in hospital wards. Doctors may assess and monitor patients' health characteristics from anywhere, and they can then administer drugs in compliance. [7] Recent advancements in IoMT, wearable sensors, and telecommunication technologies have enabled the delivery of intelligent healthcare services, making human life smarter in the age of pervasive computing. IoMT has the potential to transform the medical services business by bridging the gap between patients, medical care specialists, and caretakers using IoMT based devices, and software. Around Aided Living (AAL) makes it possible to integrate different innovations into routine activities. This research suggests an intelligent healthcare system for AAL. It displays the ongoing work of more experienced individuals using IoMT and AI computations, enabling for quicker research, better guidance, and treatment options. Wearing sensors on the subject's left ankle, right arm, and chest allows for data collection. The integrated cloud and data analytics layer receives this data, which is subsequently sent over IoMT devices. Many pieces of data can be processed simultaneously using methods like hadoop map reduce. The map reduces framework's multinomial nave baye's classifier is used to determine how different bodily parts move. The parallel processing rather than serial processing, it is more scalable and performs better. The twelve physical activities indicated by our suggested framework have an overall accuracy of 97.1%.

This is the finest choice for recognizing physical activity and remotely monitoring the health of senior citizens. The article [8], using networking technology, the IoMT, an innovative approach, links medical applications and equipment to healthcare IT systems. In this study, the IoMT approach was employed to treat orthopaedic disorders and combat the COVID-19 pandemic. IoMT offers several cloud and network-connected services, including data sharing; report monitoring, patient tracking, and medical hygiene care. During the COVID-19 lockdown, IoMT can revolutionize the healthcare industry, particularly in treating orthopaedic patients with better care and satisfaction. The proposed IoMT approach also enables remote location healthcare. IoMT has been implemented in many countries to stop the spread of COVID-19, reduce the disease's impact on human lives, protect front line staff, and decrease mortality rates. Increased security has resulted from the quick and widespread use of IoMT globally, which has also advanced technology and applications. Numerous current investigations show that secure IoMT applications can be deployed by including security features into the technology. Additionally, when new IoMT technologies are integrated with big data, blockchain, and AI, additional useful solutions can be found. This article discusses the advancements made in IoMT architecture, technologies, applications, and security to combat the COVID-19 pandemic. The study provides valuable information on various IoMT architecture models, new applications, security metrics, and technology paths used to address the challenges posed by COVID-19 [9]. The IoMT is piquing the attention of the healthcare research community. Patients are given a variety of knowledge to aid in their recuperation. However, burglars might be able to modify the addresses of a lot of medical equipment, endangering the lives of dangerous patients like those with diseases resembling brain tumours. A clump of abnormal brain cells can cause brain tumours, which can be fatal and impair the brain. The early detection of brain tumours is crucial for the diagnosis, prognosis, and treatment of these conditions. Conventional approaches for identifying cancer include biopsies and human inspection of different scans. These processes take a lot of time, are impracticable for big amounts of data, and require the radiologist's attention in order to make conclusions. Accurate disease diagnosis, information mining, and the real time necessity of the multi-access healthcare monitoring system are currently difficult processes. The most recent developments in information technology and IoMT have made it simpler for a wide number of individuals to utilise the smart system. A skilled,

round the clock medical care administration is needed for regular, reliable patient monitoring. The cloud platforms are certainly necessary in sophisticated medical care systems to meet this demand.

AI allows computers to perform tasks typically carried out by humans. In a smart healthcare system using IoMT, machines equipped with sensors can monitor health metrics of patients and interpret the data collected. AI based data transformation and interpretation approaches can be used for analysis once the medical data is received [10]. In the event of a critical situation, doctors or other medical specialists can be contacted via intelligent AI based smartphone applications [11]. In situations that are not dangerous, self-prevention techniques are possible. Additionally, people with disabilities, in particular, are better able to use a variety of smart devices to access particular household appliances thanks to quick development of new hardware and software technologies in IoMT. IoMT is composed of various computing components that operate as pro-active advocates for steadfast users. As a result, crucial components are required in IoMT in order to make wise selections. For instance, it is necessary to take into account user preferences in order to determine their choice of interest in specific circumstances [12].

3. IoMT Affecting Factors

The latest innovation in the healthcare industry is IoMT, which utilizes connected devices and cloud storage. This technology combines medical devices and IoT applications to keep healthcare providers connected with their patients. The IT systems, remote patient monitoring and other healthcare procedures can be performed. The infrastructure of medical devices makes use of radio transmission, internet access using Wi-Fi, and other networking technologies. IoMT uses connected hospital equipment, portable diagnostic equipment, and wearable sensor technology to communicate data. The IoT technologies are including device to cloud and device to device connectivity, the provision of digital health services is becoming more widely available than ever before. IoMT, often referred to as healthcare IoT, uses automation, sensors, and machine intelligence, much like standard IoT devices, to lessen the need for people to carry out standard medical procedures. Access to healthcare information is made simple for patients and their caregivers via sensor based processes. IoMT reduces the necessity of going to a hospital or doctor's office. IoMT's cost cutting strategies benefit both patients and providers. The most common factors of IoMT are shown in Figure 2 and the hierarchy of factors and alternatives are shown in Figure 3.

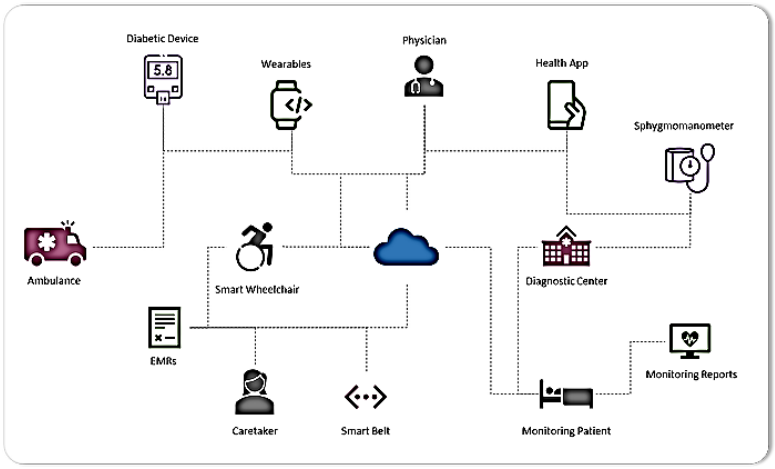

Fig. 2. IoMT representing factors [13]

3.1 Getting Complete Understanding of End Users [G1]

In the world of IoMT, the use of interconnected medical devices is expected to rise as more healthcare providers embrace value based care models. It relies heavily on patient information and insights. Adopting and integrating connected medical devices, on the other hand, presents a number of challenges, including their IT infrastructure's capacity to handle the data and connections, as well as convincing clinicians and patients of the devices' safety and effectiveness. To overcome these challenges, organisations should have a thorough understanding of their end-clients and promote plans of action and scenarios that demonstrate how their goods may perform quietly and provide an incentive for key partners in the medical services framework [13].

3.2 Creating New Funding, Business, and Operating Models [G2]

As health care organisations place a greater emphasis on cost reduction and treatment quality improvement, organizational companies are required to give more proof of the added value of new and better goods. According to a survey, several industry groups are demonstrating the value of their related medical devices. Some of them provide services rather than tangible goods. The distinct types of development will call for distinct strategies, and advancement

won't necessarily be predetermined, thanks to trend setters coming up with creative wagering and prize-expanding techniques as well as improving current public and private installation frameworks [14].

3.3 Understanding Requirements for Interoperability [G3]

The biggest challenge for the medical technology industry is to adhere to national and international standards and protocols for exchanging and using data. In addition, creating an integrated governance system and obtaining permission to access healthcare data are two other technological challenges. To achieve successful interoperability, open platforms based on open data standards should be used. Data will be easier to access for each other if payers, providers, and technology companies collaborate [15].

3.4 Maintaining Cyber-Security [G4]

Due to the increasing availability and sophistication of linked medical devices, which offer new risks to data security, Organization is beset by cyber security problems. Costs and scope of breaches are typically high and vast. In our study, four out of five respondents said they were ready to handle cybersecurity concerns for their devices. However, additional research indicates that a large number of stakeholders are unaware of these risks, how to avoid them, and what to do if one is discovered. Since cybersecurity risks cannot be totally removed, stakeholders must cooperate and develop a proactive risk management approach. Associations should combine security methods including "security by configuration," "continuous monitoring," "digital danger demonstrating and investigation," and "danger moderation and remediation" [16].

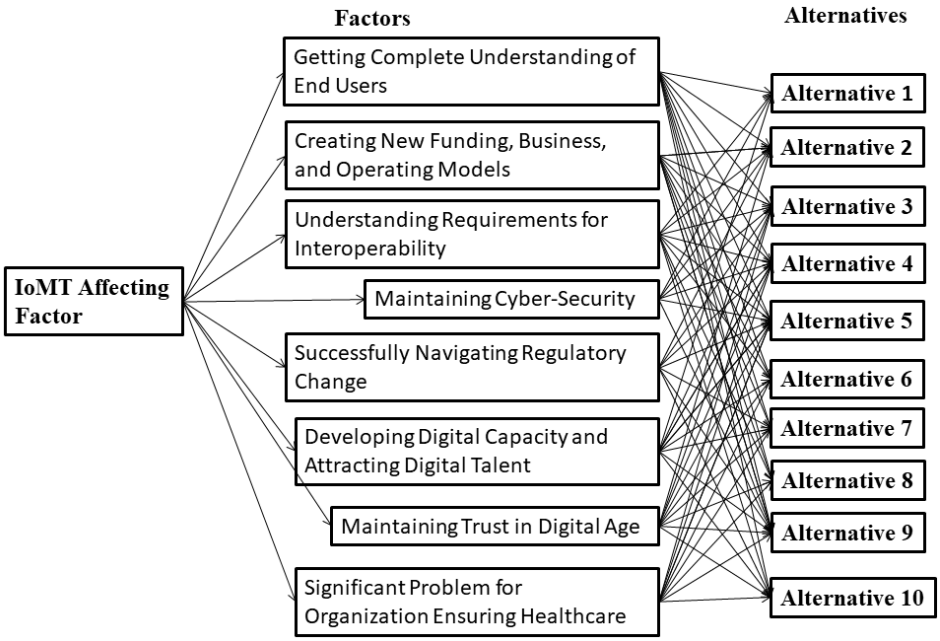

Fig. 3. Hierarchy of IoMT affecting factors

3.5 Successfully Navigating Regulatory Change [G5]

To ensure the success of the IoMT and connected medical devices, it is crucial for organizations to navigate regulatory changes, especially the new rules in the US and Europe. To do so, companies must adopt a proactive and well planned strategy. They must communicate with controllers, incorporate physicians and patients in product development, and ensure the sustainability of their development system.

3.6 Developing Digital Capacity and Attracting Digital Talent [G6]

The adoption of IoMT solutions is being delayed by a rising skills gap, which is causing key stakeholders to express increased worry. Association organisations should hire information researchers and other people with varied backgrounds who have strong creative and logical underpinnings if they want to continue to be taken seriously. It will be essential to collaborate and build relationships with a broad range of planned and anticipated affiliations, including academics, information first tech organisations, and creative new enterprises, in order to develop this expertise [17].

3.7 Maintaining Trust in Digital Age [G7]

While established medical device businesses engage more in data management and analytics, global technology companies and newcomers to the healthcare sector are getting more active in the connected medical device market. For organization companies to gain trust from patients, the public and healthcare professionals regarding the responsible use and protection of data, they must demonstrate this clearly as they create services and strategies that involve the transfer

of patient data. Companies that develop medical technology must also set fundamental rules for permission and data management that allow patients control over their own data and the choice not to share it [12].

3.8 Significant Problem for Organization Ensuring Healthcare [G8]

There is a need to demonstrate the added value of linked medical devices to both clinicians and patients to improve healthcare outcomes and economics. However, there are challenges such as the lack of governance norms and convincing proof of cost-effectiveness of these devices, and how they can support the agenda. To overcome these challenges, the devices should be user-friendly and intuitive, and staff should receive adequate support and training to use the technology effectively [7].

4. Methodology (Hybrid Multi Criteria Decision Making Methodology)

We used a combination of two decision making AI tools, FAHP and FTOPSIS, along with soft computing or AI techniques, to evaluate the security aspects of IoMT [18]. We gathered data from the literature and used a multi-model, distinctive, conventional approach to evaluate the elements affecting IoMT. FAHP was used to measure the component weight, and FTOPSIS determined where the factors should fall in relation to the other possibilities [19]. To evaluate the factors quantitatively, we used the fuzzy system. However, FAHP has limitations, so we merged FTOPSIS with a management strategy to manage hybrid FAHP and FTOPSIS [20]. This approach helped to accurately assess the impact factor and its alternative.

4.1 Fuzzy AHP Methodology

The FAHP method is used to determine the best solutions for security issues in IoMT by considering attributes and related options. Fuzzy numbers are used to assess and rank the evaluation processes. Table 1 shows the fuzzy numbers used to compare the philological rankings [18].

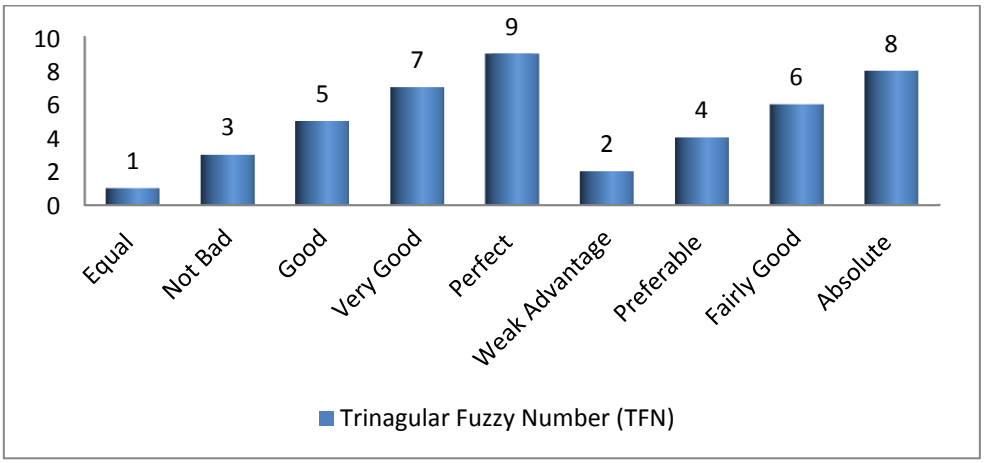

Fig. 4. Fuzzy comparison measures (FCM)

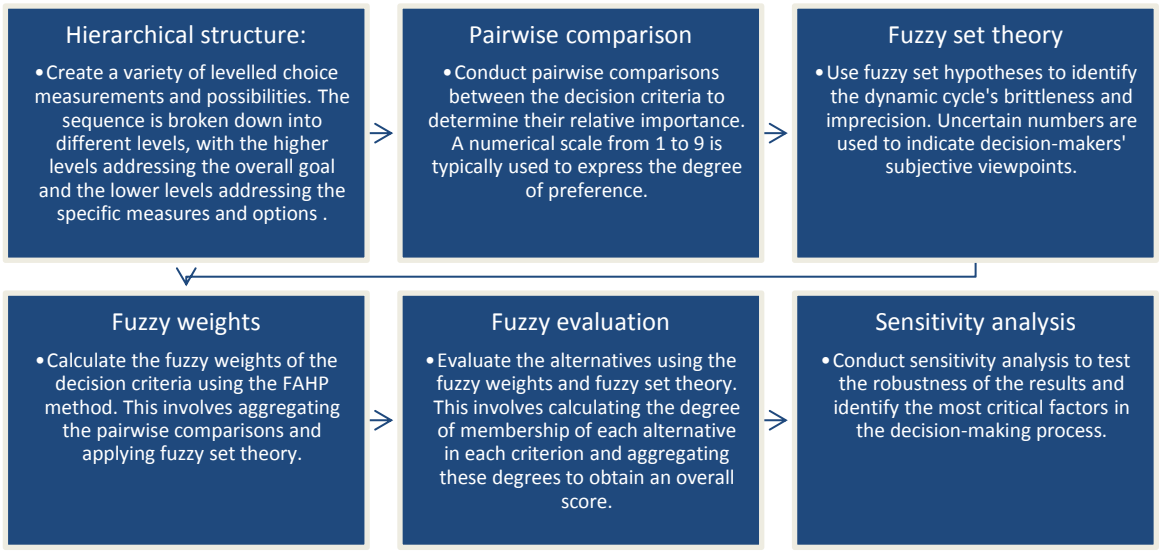

Fig. 5. Process diagram of fuzzy-AHP

FAHP method evaluates each element submitted by the examiner and selects Fuzzy Comparison Measures (FCM) or TFN from a hierarchical structure to make improvements [18]. The TFN values are represented by the Figure 4. Each variable has a pair-wise relationship that determines its importance to the whole. The next step is to use fuzzy correlation measurements to change the numerical value of the linguistic phrases. Finally, the FAHP technique is used to determine the weight of the elements [21]. The process is explained below in Figure 5, and the mathematical process of Fuzzy-AHP from appendix A.

4.2 Fuzzy-TOPSIS

The TOPSIS approach is used in multi-criteria decision-making to rank choices based on their geometrical layout. The approach entails assessing how distant each choice is from the positive ideal solution, which is the most desired outcome, and the negative ideal solution, which is the least desirable outcome. This allows you to easily evaluate the alternatives based on how distant they are from the greatest possibilities. In order to add fuzzy logic into the process, fuzzy numbers are allocated to the criterion to signify their relevance and preferences. FTOPSIS is especially useful about the model's values or the loads assigned to the measurements [22]. The leader might indicate their level of conviction or doubt about the traits by using fuzzy numbers to address the measurements esteems. The AI technique of FTOPSIS steps are shown in Figure 6.

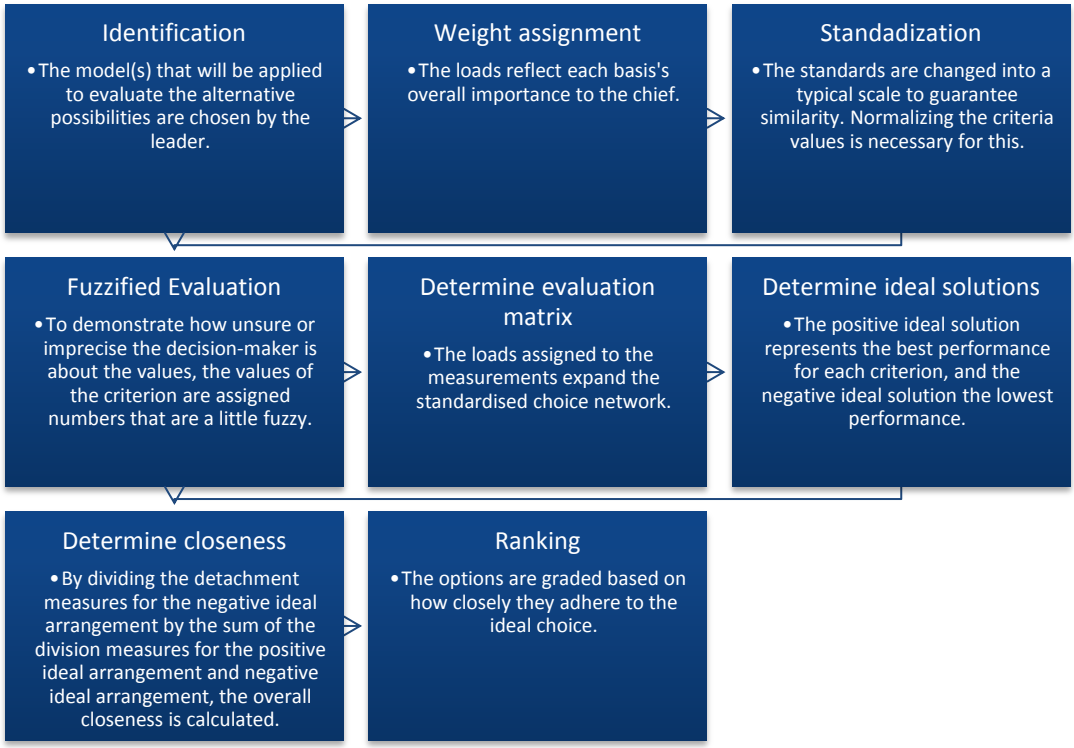

Fig. 6. Process Diagram of Fuzzy-TOPSIS

5. Numerical Data Analysis

The hybrid FAHP and FTOPSIS approach of AI combines both algorithms. FAHP determines the weight of the influencing variables (G1-G8), and FTOPSIS evaluates the ranking of the alternatives (H1-H10). Because it is difficult to quantify the impact of factors in IoMT, subjective evaluation is commonly used. The property at one level can have different impacts on properties at higher levels. Table 1, are formulated by the different steps of FAHP. To facilitate assessment, a hierarchy of the aggregated attributes is built. The degree of closeness is shown in Figure 8. Table 2, is the result of closeness coefficient. It evaluates the level of closeness between alternatives.

Table 1. Evaluated weight of the factors

Factors	Evaluated weights	Best Non Fuzzy Performance	Ranking
G1	0.150000, 0.180000, 0.210000	0.160000	02
G2	0.190000, 0.200000, 0.220000	0.190000	01
G3	0.130000, 0.160000, 0.190000	0.150000	04
G4	0.120000, 0.150000, 0.180000	0.160000	03
G5	0.060000, 0.080000, 0.100000	0.070000	08
G6	0.070000, 0.090000, 0.130000	0.090000	06
G7	0.080000, 0.100000, 0.130000	0.100000	05
G8	0.050000, 0.080000, 0.120000	0.080000	07

Table 2. Closeness coefficients to aspired level among different alternatives

Alternatives	dþi	di	Gaps degree of CCþi	Satisfaction degree of CCi
H1	0.2400	0.4900	0.6700	0.3300
H2	0.8200	0.9000	0.7800	0.2200
H3	0.2700	0.5100	0.6500	0.3500
H4	0.3200	0.4800	0.6000	0.4000
H5	0.4200	0.6100	0.5900	0.4100
H6	0.2700	0.3000	0.5200	0.4800
H7	0.3000	0.4200	0.5800	0.4200
H8	0.4200	0.5300	0.5500	0.4500
H9	0.2900	0.4200	0.5900	0.4100
H10	0.3000	0.5800	0.6500	0.3500

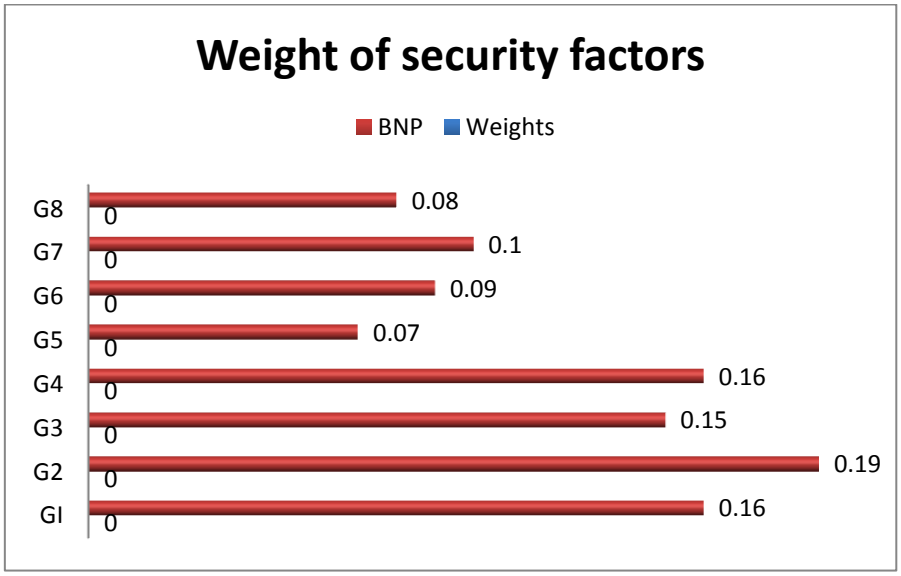

Fig. 7. Weight of the security factors in IoMT

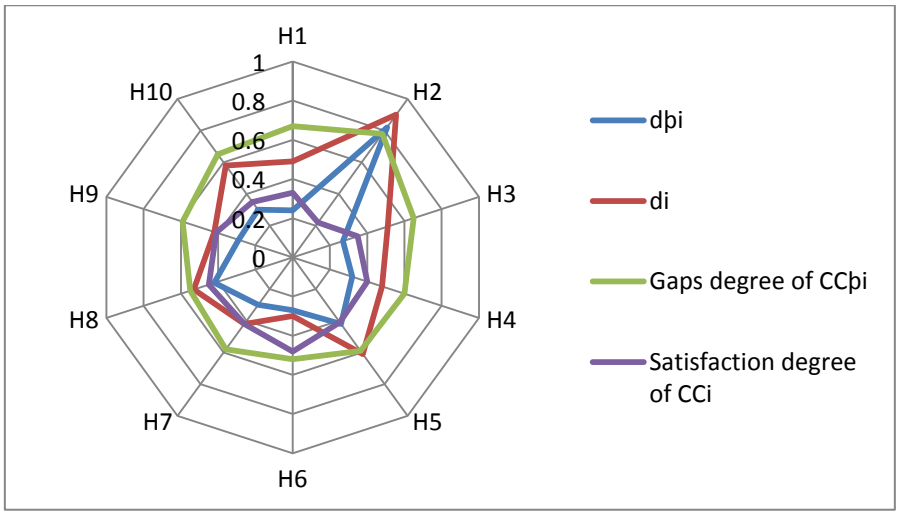

Fig. 8. Degree of closeness IoMT

6. Comparison

For the same information, different procedures can produce different results. Various methodologies are used to assess the dependability and viability of a procedure. The precision and effectiveness of the outcomes were assessed using the AI method.

Table 3. The result of usual/classical method and FAHP and FTOPSIS method

Approach	H1	H2	H3	H4	H5	H6	H7	H8	H9	H10
Fuzzy-AHP-TOPSIS	0.331200	0.222400	0.352500	0.405500	0.414700	0.484900	0.425600	0.455100	0.416100	0.358900
Classical-AHP-TOPSIS	0.325600	0.222500	0.356100	0.405800	0.415600	0.485800	0.429800	0.466000	0.408900	0.347800

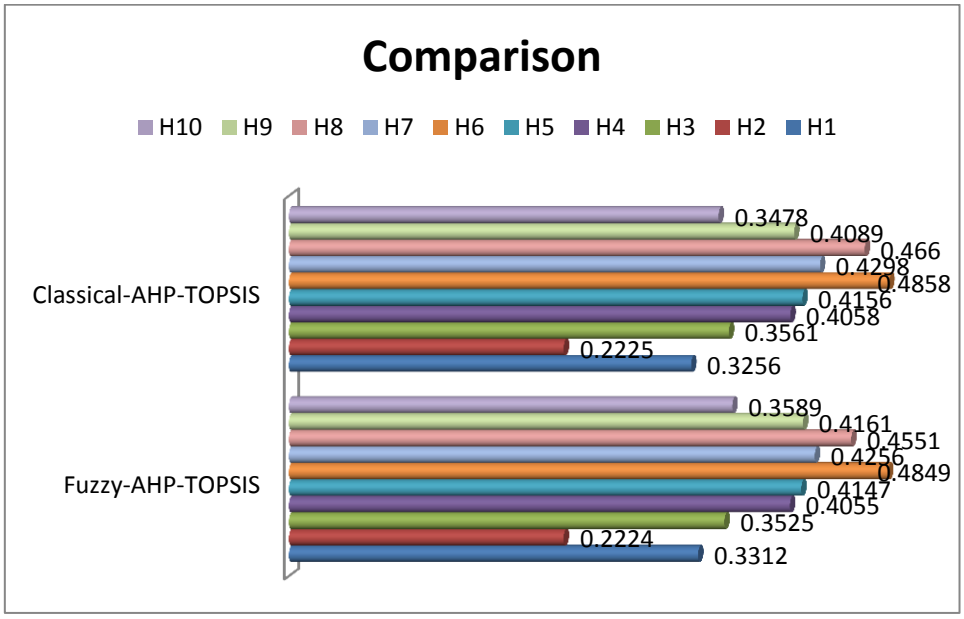

Fig. 9. Comparison of IoMT Alternatives with the Fuzzified and Non-Fuzzified Approach

The AHP-TOPSIS technique gathers and analyses data in the same way as the Fuzzy AHP-TOPSIS method, but no fuzzifications is used. Thus, in conventional AHP-TOPSIS, real number characteristics are applied. Table 3 and Figure 9 present the analysis of the fluff and regular AHP-TOPSIS finds. The Pearson correlation between the F-AHP-TOPSIS technique and the conventional AHP-TOPSIS method is 0.999176, which denotes a substantial association. The FAHP and FTOPSIS procedures are therefore more trustworthy and efficient than the conventional AHP-TOPSIS approach.

7. Sensitivity Analysis

A responsiveness assessment is undertaken to examine the influence of variables on outcomes. Table 4 shows the sensitivity analysis of the variable weights. The sensitivity analysis in our IoMT study is performed by repeating the same number of trials on several occasions for each component. The contentment degree (CC-i) is estimated using the AI approach by maintaining the weight of each component (G1 to G8) constant. Table 4 presents the results of the testing of awareness. Table 4 and Figure 7 both show the beginning weight in the primary column. The primary set of data is displayed in the main line of Figure 7. The Factor-8 (G1 to G8) is very pleased (CC-i), according to the original weights and results. From experiment A1 to experiment A10, ten trials are conducted. Component 8 (G1 to G8) truly has a high fulfilment degree (CC-I), according to the findings of eight tests. Additionally, H2 is the section that carries the least weight in any preliminary. Results that differ from one another suggest that decision assessments are sensitive to heaps. The graphical representation of sensitivity analysis is depicted in Figure 10.

Table 4. Sensitivity Analysis

Alternative	H1	H2	H3	H4	H5	H6	H7	H8	H9	H10
Weight	0.331200	0.222400	0.35250	0.405500	0.41470	0.484900	0.425600	0.455100	0.416100	0.358900
G1	0.352300	0.237500	0.367100	0.421300	0.420600	0.496300	0.431790	0.471000	0.429400	0.3697900
G2	0.330000	0.227500	0.354100	0.409800	0.411100	0.495800	0.426800	0.461500	0.428900	0.364800
G3	0.333600	0.22200	0.361100	0.403800	0.406600	0.494300	0.423800	0.457000	0.427400	0.361800
G4	0.342600	0.044500	0.348500	0.393900	0.41580	0.48530	0.427100	0.466200	0.418400	0.365100
G5	0.303800	0.189900	0.315300	0.378600	0.374200	0.456500	0.392100	0.424600	0.389600	0.330100
G6	0.256500	0.140900	0.270500	0.335300	0.327800	0.412800	0.404800	0.378200	0.345900	0.342800
G7	0.348300	0.227800	0.360300	0.428200	0.416000	0.501500	0.434800	0.466400	0.434600	0.372800
G8	0.332900	0.239500	0.358100	0.413800	0.422900	0.486400	0.428800	0.473300	0.419500	0.366800

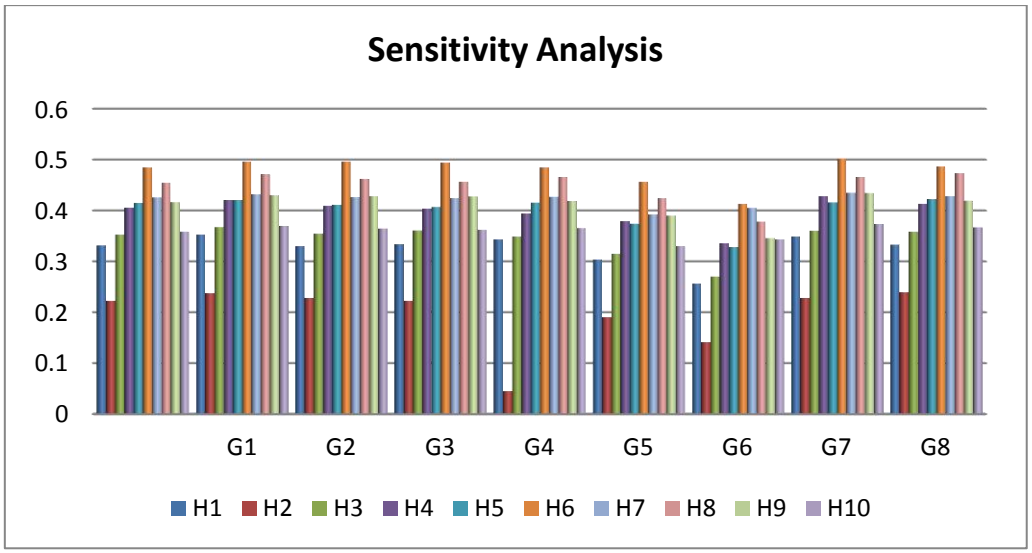

Fig. 10. Graphical representation of sensitivity analysis

8. Results

The Hybrid FAHP and FTOPSIS approach of AI are used to evaluate the influencing variables of IoMT, and it is considered the most important method for assessing IoMT factors. The focus of this study is to ensure the security and sustainability of the healthcare industry. As IoMT applications become more prevalent, their utilization and complexity are increasing. Due to the exponential expansion of security concerns, the creation of highly secure and supportable electronic submissions for the healthcare business is required. The most effective strategies to achieve attainable security are security assessment and assessment. This study evaluates and coordinates the security and maintainability elements in the context of IoMT. The test findings will help developers integrate online secure IoMT into their development. In this study, we selected ten IoMT based application alternatives based on experts' opinions regarding their contributing risk plan, mitigation strategy, and security features.

The quantitative findings provided by FAHP and FTOPSIS will assist professionals in categorising higher-ranking IoMT framework components. The FAHP approach assigns a weight to the risk attributes; FTOPSIS method assigns a position to the associated credits. When FAHP and FTOPSIS are compared to standard AHP TOPSIS, the methodologies improve. Sensitivity analysis is used to assess the amount of IoMT satisfaction. This evaluation can give improvement rules to aid developers in fine-tuning the security structure by utilising highly organised factors linked to IoMT. According to the presentation, IoMT structure evaluation is vital and active in its own right. Taking everything into consideration, this assessment may have certain limits that may be solved with more study. The following are examples: A substantial quantity of information has been acquired for website architecture. The findings may alter if there is a large amount of data. Additional security configuration factors may exist in addition to those identified in this work.

9. Conclusion

This in depth investigation of the IoMT focuses on the many enabling approaches used in Smart Healthcare Systems. This article discusses factor estimation, soft computing methodologies, artificial intelligence, and other Smart Healthcare System concepts. This research illustrates and distinguishes the many IoMT architectures utilised by several writers for frameworks for outstanding medical services based on artificial intelligence. When a fantastic medical services framework uses trustworthy information, it can function perfectly. We use embedded or wearable IoMT devices to collect clinical data on the patient's body. The energy efficiency of IoMT devices influences their size, durability, and utilisation. As a result, our key focus is on the energy optimisation tactics of the IoMT device. This research thoroughly examines each creator's most recent efforts to maintain an IoMT organization's energy proficiency. Energy use, bundle delivery proportion, battery life expectancy type of management, power channel, network throughput, inertness, transmission rate, and other factors all affect how effective a system is. It is considered that there are several linkages between IoMT variables. Utilising the FAHP and FTOPSIS method is to dissect the accuracy and feasibility of the IoMT-based medical services architecture. We also discuss the IoMT framework's main health categories. The patient's normal body improvement, change in the temperature of the prosperity noticing device, energy efficiency of the association, transmission range of the device, execution of the IoMT contraption in a heterogeneous environment, nature of organisation, and security are the eight significant issues examined in this paper that should be taken into account when implementing an IoMT network-based splendid clinical consideration system. The principal

barrier to increasing energy efficiency has just been contrasted and examined; six more barriers need to be researched in the future. Because medical data is so sensitive, the system must be thoroughly examined and improved in the future.

Ethical Approval: This is an observational study. There is no ethical approval required.

Competing Interests: The authors have no competing interests to declare that are relevant to the content of this article.

Authors' contributions: All the authors have contributed equally to the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: There is no funding.

Availability of data and materials: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to government data policy.

References

[1] N. Homer *et al.*, "HIPAA, the Privacy Rule, and Its Application to Health Research," *PLoS Genet.*, vol. 4, no. 8, Aug. 2009, doi: 10.1371/JOURNAL.PGEN.1000167.

[2] L. P. Verma and M. Kumar, "An IoT based Congestion Control Algorithm," *Internet of Things*, vol. 9, p. 100157, Mar. 2020, doi: 10.1016/J.IOT.2019.100157.

[3] U. K. Lilhore *et al.*, "Design and Implementation of an ML and IoT Based Adaptive Traffic-Management System for Smart Cities," *Sensors 2022, Vol. 22, Page 2908*, vol. 22, no. 8, p. 2908, Apr. 2022, doi: 10.3390/S22082908.

[4] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, pp. 1–22, Dec. 2019, doi: 10.1186/S42400-019-0038-7/FIGURES/8.

[5] G. Thamilarasu, A. Odesile, and A. Hoang, "An intrusion detection system for internet of medical things," *IEEE Access*, vol. 8, pp. 181560–181576, 2020, doi: 10.1109/ACCESS.2020.3026260.

[6] J. Almalki *et al.*, "Enabling Blockchain with IoMT Devices for Healthcare," *Inf. 2022, Vol. 13, Page 448*, vol. 13, no. 10, p. 448, Sep. 2022, doi: 10.3390/INFO13100448.

[7] L. Syed, S. Jabeen, M. S., and A. Alsaeedi, "Smart healthcare framework for ambient assisted living using IoMT and big data analytics techniques," *Futur. Gener. Comput. Syst.*, vol. 101, pp. 136–151, Dec. 2019, doi: 10.1016/J.FUTURE.2019.06.004.

[8] R. Pratap Singh, M. Javaid, A. Haleem, R. Vaishya, and S. Ali, "Internet of Medical Things (IoMT) for orthopaedic in COVID-19 pandemic: Roles, challenges, and applications," *J. Clin. Orthop. Trauma*, vol. 11, no. 4, pp. 713–717, Jul. 2020, doi: 10.1016/J.JCOT.2020.05.011.

[9] S. R. Khan, M. Sikandar, A. Almogren, I. Ud Din, A. Guerrieri, and G. Fortino, "IoMT-based computational approach for detecting brain tumor," *Futur. Gener. Comput. Syst.*, vol. 109, pp. 360–367, Aug. 2020, doi: 10.1016/J.FUTURE.2020.03.054.

[10] P. Savadjiev *et al.*, "Demystification of AI-driven medical image interpretation: past, present and future," *Eur. Radiol.*, vol. 29, no. 3, pp. 1616–1624, Mar. 2019, doi: 10.1007/S00330-018-5674-X/TABLES/2.

[11] A. K. Rangarajan and H. K. Ramachandran, "A preliminary analysis of AI based smartphone application for diagnosis of COVID-19 using chest X-ray images," *Expert Syst. Appl.*, vol. 183, p. 115401, Nov. 2021, doi: 10.1016/J.ESWA.2021.115401.

[12] A. Ferrag, I. A. Jayaraj, B. Shanmugam, S. Azam, and G. N. Samy, "A Systematic Review of Radio Frequency Threats in IoMT," *J. Sens. Actuator Networks 2022, Vol. 11, Page 62*, vol. 11, no. 4, p. 62, Sep. 2022, doi: 10.3390/JSAN11040062.

[13] "Top 5 Factors Affecting the Performance of IoMT Devices." https://www.citiustech.com/blog/top-5-factors-affecting-the-performance-of-iomt-devices (accessed Dec. 13, 2022).

[14] C. H. Yang, Y. Y. Liu, C. H. Chiang, and Y. W. Su, "National IoMT platform strategy portfolio decision model under the COVID-19 environment: based on the financial and non-financial value view," *Ann. Oper. Res.*, p. 1, 2022, doi: 10.1007/S10479-022-05016-4.

[15] R. Dwivedi, D. Mehrotra, and S. Chandra, "Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review," *J. Oral Biol. Craniofacial Res.*, vol. 12, no. 2, p. 302, Mar. 2022, doi: 10.1016/J.JOBCR.2021.11.010.

[16] I. V. Pustokhina, D. A. Pustokhin, D. Gupta, A. Khanna, K. Shankar, and G. N. Nguyen, "An Effective Training Scheme for Deep Neural Network in Edge Computing Enabled Internet of Medical Things (IoMT) Systems," *IEEE Access*, vol. 8, pp. 107112–107123, 2020, doi: 10.1109/ACCESS.2020.3000322.

[17] M. Ahmad *et al.*, "Healthcare device security assessment through computational methodology," *Comput. Syst. Sci. Eng.*, vol. 41, no. 2, 2022, doi: 10.32604/csse.2022.020097.

[18] R. W. Saaty, "The analytic hierarchy process—what it is and how it is used," *Math. Model.*, vol. 9, no. 3–5, pp. 161–176, Jan. 1987, doi: 10.1016/0270-0255(87)90473-8.

[19] F. A. Alzahrani, M. Ahmad, M. Nadeem, R. Kumar, and R. A. Khan, "Integrity Assessment of Medical Devices for Improving Hospital Services," *Comput. Mater. Contin.*, vol. 67, no. 3, p. 3619, Mar. 2021, doi: 10.32604/CMC.2021.014869.

[20] H. Alyami *et al.*, "The evaluation of software security through quantum computing techniques: A durability perspective," *Appl. Sci.*, vol. 11, no. 24, 2021, doi: 10.3390/app112411784.

[21] T. L. Saaty, "A scaling method for priorities in hierarchical structures," *J. Math. Psychol.*, vol. 15, no. 3, pp. 234–281, Jun. 1977, doi: 10.1016/0022-2496(77)90033-5.

[22] M. Alenezi, A. Agrawal, R. Kumar, and R. A. Khan, "Evaluating Performance of Web Application Security through a Fuzzy Based Hybrid Multi-Criteria Decision-Making Approach: Design Tactics Perspective," *IEEE Access*, vol. 8, pp. 25543–25556, 2020, doi: 10.1109/ACCESS.2020.2970784.

Authors' Profiles

Mohd Nadeem is currently working as an Assistant Professor in School of Computer Applications at Babu Banarasi Das University, Lucknow, UP, India. I have 8+ Year experience of Teaching and research. I have Submitted PhD from the Department of Information Technology, Babasaheb Bhimrao Ambedkar University (A Central University), 4 Lucknow, India. I also worked as a faculty in Department of UIET, BBAU Lucknow since 2014 to 2019. I completed M-Tech from Integral University, Lucknow, India in 2013. I completed B-Tech from Chandrasekhar Azad University Kanpur, India in 2010. My research interests are in the areas of Quantum Software Security, Quantum Security, Network Security, Security Risk, IoT Security, and Quantum Computing Security, Big Data Analytics, and Artificial Intelligence.

Prabhash Chandra Pathak is currently working as an Associate Professor and Head in School of Computer Applications at Babu Banarasi Das University, Lucknow, UP, India. The research interests are in the areas of Software Security, Fuzzy Logic, Blockchain technology, Security Risk, IoT Security, Big Data Analytics, and Artificial Intelligence.

Mahfooz Ahmad received the B.Tech, degree in Electronics and Communication Engineering from AKT University, and the M.Tech degree in Electronic Circuits and Systems from Integral University. He is currently working as an Assistant Professor in the Department of Electronics and Communication Engineering at Integral University. His research areas include HDLC Controller Using VHDL, Digital Image Processing, Solar PV Maximum Power Tracking System AI, Soft computing. He has published 11 research papers in International and IEEE Conference Paper and 01 Patent paper.

Masood Ahmad received the B.Tech, M.Tech degree in information technology from AKTU, Lucknow, and pursuing the philosophy of doctorate degree in information technology from Babasaheb Bhimrao Ambedkar University, respectively. He is currently working as an Assistant Professor, Head of department at the Department of Computer science & Engineering, Faculty of Azad Institute of Engineering & Technology. His research areas include Medical Device security, AI, Soft computing, and mobile network analysis. He has published 26 research papers in SCI, SCIS and ESCI and two books are also published.

How to cite this paper: Mohd. Nadeem, Prabhash Chandra Pathak, Mahfooz Ahmad, Masood Ahmad, "Determination of Security Factors Affecting Internet of Medical Things by Artificial Intelligence Technique", International Journal of Education and Management Engineering (IJEME), Vol.14, No.2, pp. 41-52, 2024. DOI:10.5815/ijeme.2024.02.04