Hindawi
Security and Communication Networks
Volume 2020, Article ID 8829595, 14 pages
https://doi.org/10.1155/2020/8829595

Research Article

Evaluating Security of Internet of Medical Things Using the Analytic Network Process Method

Xucheng Huang[1] **and Shah Nazir**[2]

[1]*School of Finance, Shanghai Lixin University of Accounting and Finance, Shanghai 201209, China*
[2]*Department of Computer Science, University of Swabi, Swabi, Pakistan*

Correspondence should be addressed to Xucheng Huang; huangxucheng@lixin.edu.cn

Received 23 June 2020; Revised 2 July 2020; Accepted 24 July 2020; Published 1 September 2020

Academic Editor: Amir Anees

Internet of Medical Things (IoMT) plays an important role in healthcare. Different devices such as smart sensors, wearable devices, handheld, and many other devices are connected in a network in the form of Internet of Things (IoT) for the smooth running of communication in healthcare. Security of these devices in healthcare is important due to its nature of functionality and efficiency. An efficient and robust security system is in dire need to cope with the attacks, threats, and vulnerability. The security evaluation of IoMT is an issue since couple of years. Therefore, the aim of the proposed study is to evaluate the security of IoMT by using the analytic network (ANP) process. The proposed approach is applied using ISO/IEC 27002 (ISO 27002) standard and some other important features from the literature. The results of the proposed research demonstrate the effective IoMT components which can further be used as secure IoMT.

1. Introduction

Internet of Things has several applications in the daily life and has made life very easy. From industry to education, healthcare, and other places, the IoT is mostly used. Internet of Medical Things is the advanced version of IoT which has a key role in healthcare. Devices such as wearable, handheld, sensors, actuator, and others are connected for communication through Internet. For the smooth communication of these devices, security is important to run in an effective and efficient way. Security is the protection from unauthorized access of illegal users. In healthcare, the devices are sometimes connected through heterogeneous environment with the support of different IoT devices. So, the security evaluation is important for them to ensure that the communication is safe and secure. IoMT plays an important role in remote exchange data processes. The IoT devices have limited capabilities due to low processing, tiny memory, and limited storage, so implementing security will be a challenging task. The security and privacy in IoMT devices are vital due to a number of reasons as IoMT devices are ubiquitous and their applications are employed in health. For this purpose, reinforcing a security mechanism is indispensable to cope with these attacks, vulnerabilities, and security and privacy challenges. Security can be one of the important factors for IoHT [1–6].

The existing research regarding the security of IoMT covers different aspects. However, there is a lack of knowledge that how to evaluate the security of IoMT based on security attributes and features. So, to overcome this limitation, the proposed research presents the ANP approach for the evaluation of security of IoMT in term of the ISO/IEC 27002 (ISO 27002) standard, and some other important features identified from the literature. The ANP method incorporates the criteria given for achieving the goal based on the available alternatives. This method helps in situation when complexity arises.

The organization of the paper is as follows: Section 2 presents the related work to the security evaluation of IoMT, along with the existing approaches for security evaluations are discussed. In Section 3, the research method is briefly described. Section 4 concludes the paper.

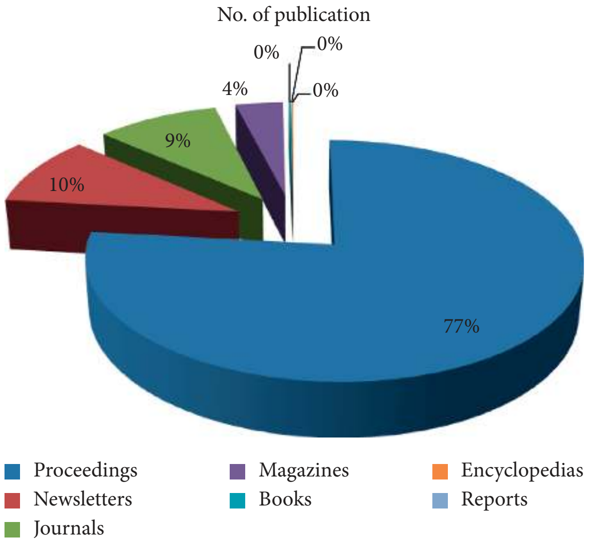


Figure 1: Type of publications along with the total number of papers.

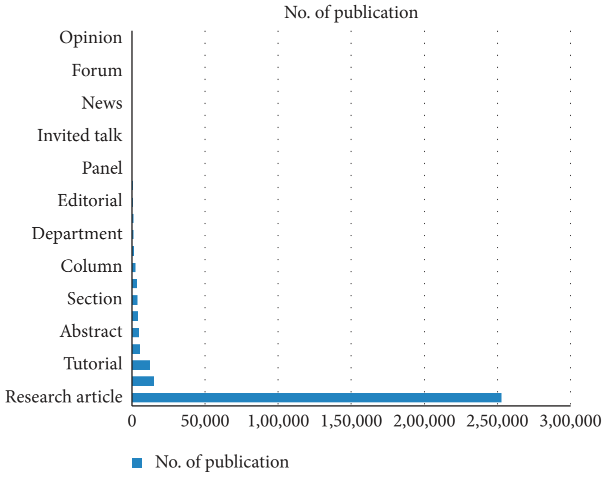


Figure 2: Content type along with the total number of publications.

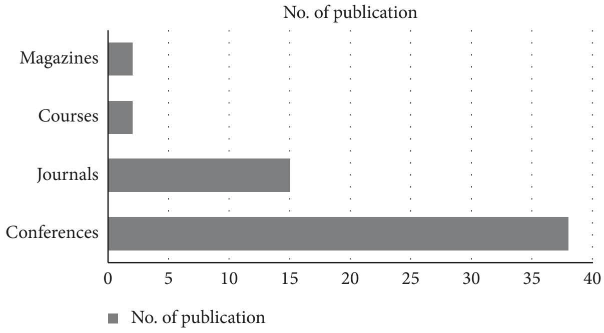


Figure 3: Type of publication with the total number of papers.

2. Related Work

Several approaches have been used by researchers for the evaluation security. The basic security requirements are defined in confidentiality, integrity, and availability (the CIA model) [7–12]. The IoMT devices are vulnerable to several threats of security, attacks, and vulnerabilities. IoMT devices suffer from enormous security threats due to low cost and power unlike traditional desktop and mobile devices. The malware can replicates itself by compromising the

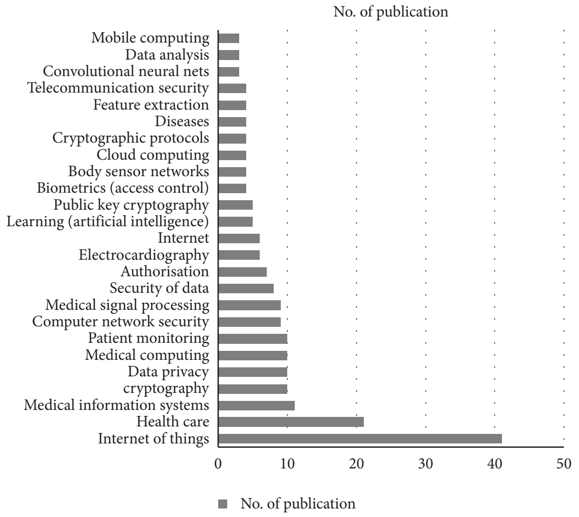


Figure 4: Publication topic with the number of papers published.

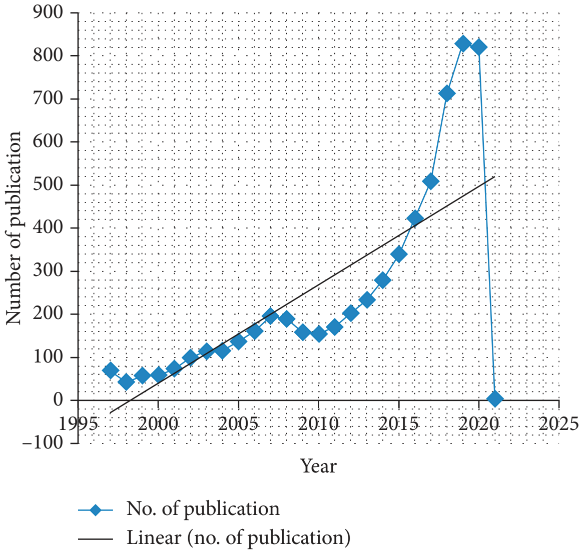


Figure 5: Number of papers published in the given year.

connection that links IoT devices [13]. Different frameworks, models, reviews, surveys, and analysis pertaining to the security of IoT-based systems for security analysis are used. Frustaci et al. [14] evaluated IoT security issues at three different layers of IoT such as perception, transportation, and application. Leister et al. [15] evaluated the security of IoT in e-health by presenting a scenario-based framework. Alrawi et al. [16] proposed component-based analysis such as IoT device, mobile application, communication channel, and cloud end points for the home-based IoT system. Tekeoglu and Tosun [17] presented a layer-based packet capturing framework for investigating security and privacy of IoT devices. Cherneyshev and Hannay [18] evaluated IoT security by using two smart TVs against the multisurface attacks. Ali and Awad [19] assessed the security of IoT smart home in terms of vulnerability. Mazhelis and Tyrväinen [20] evaluated IoT platforms from application provider perspectives. Apart from these approaches, several other approaches are being available in the literature [21–24].

Similarly, mobile computing services can be used in IoT by using services of mobile phones and apps or through the M-Health care system. The M-Health contributes to the IoT by furnishing various services such as compactness, IP connectivity, consumption of low power, and security [25]. Recently, many applications have been developed to deliver mobile-based services to the users in healthcare. The applications of smart phone enable the patients to know about their diseases after the analysis in the field of gynaecology and paediatrics [26].

The purpose of this section is to study the existing literature to know about the work done in the area of security evaluation. For this purpose, the popular libraries including ACM, IEEE, ScienceDirect, and Springer were searched. Different types of information were obtained, and the details

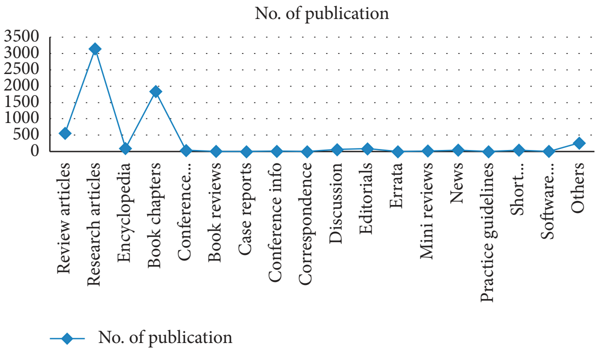


Figure 6: Number of publication and article type.

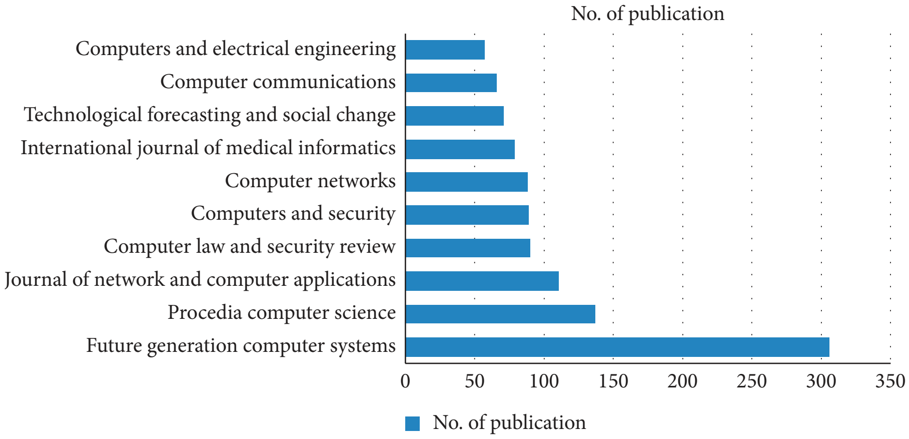


Figure 7: Publication title along with the number of papers.

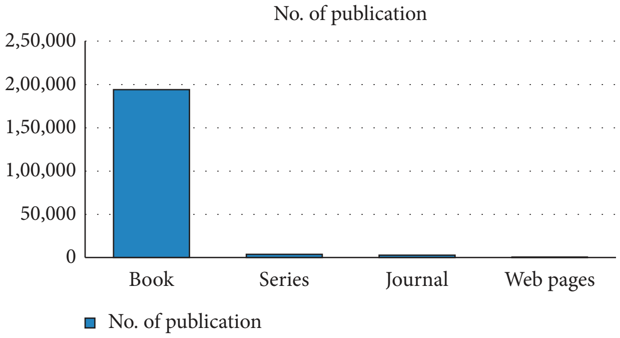


Figure 8: Number of publication with the type of publication.

are given in figures and tables in this section. Figure 1 shows the type of publication along with the total number of papers published in the ACM library.

Figure 2 shows the content type along with the total number of publications.

The purpose of searching different libraries was to know more about the research done in the area. For this purpose, the IEEE library was also searched. Figure 3 shows the type of publication along with the total number of papers published in the IEEE library.

Figure 4 shows the publication topic in the area along with the total number of papers published.

The library of ScienceDirect was also searched to know about the security-related work published in the area. Figure 5 shows the total number of publications in the given year in the ScienceDirect library.

Figure 6 shows the number of publications along with the type of publication.

Figure 7 shows the publication title along with the number of publications.

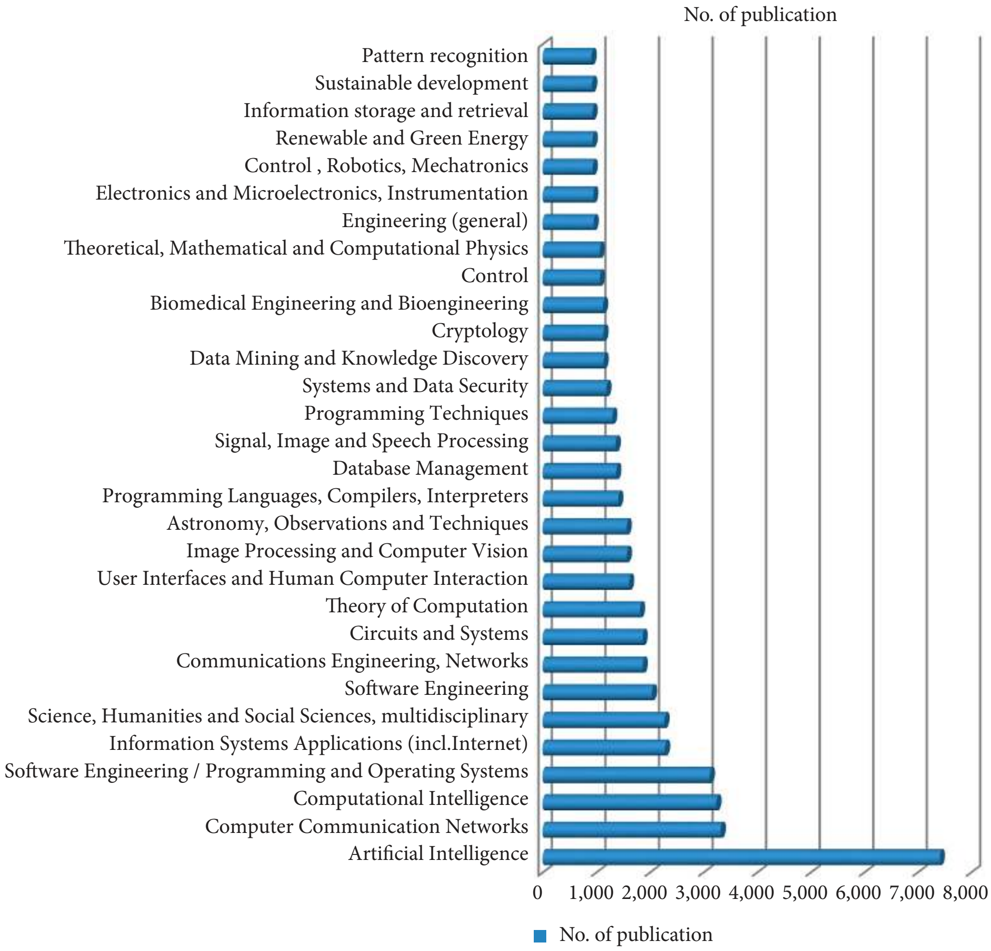


FIGURE 9: Publication topic along with the number of publications.

TABLE 1: Random consistency index.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
RI	0	0	0.58	0.9	1.12	1.24	1.32	1.41	1.45	1.49	1.51	1.48	1.56	1.57	1.59

The value of CR should be less than 0.1.

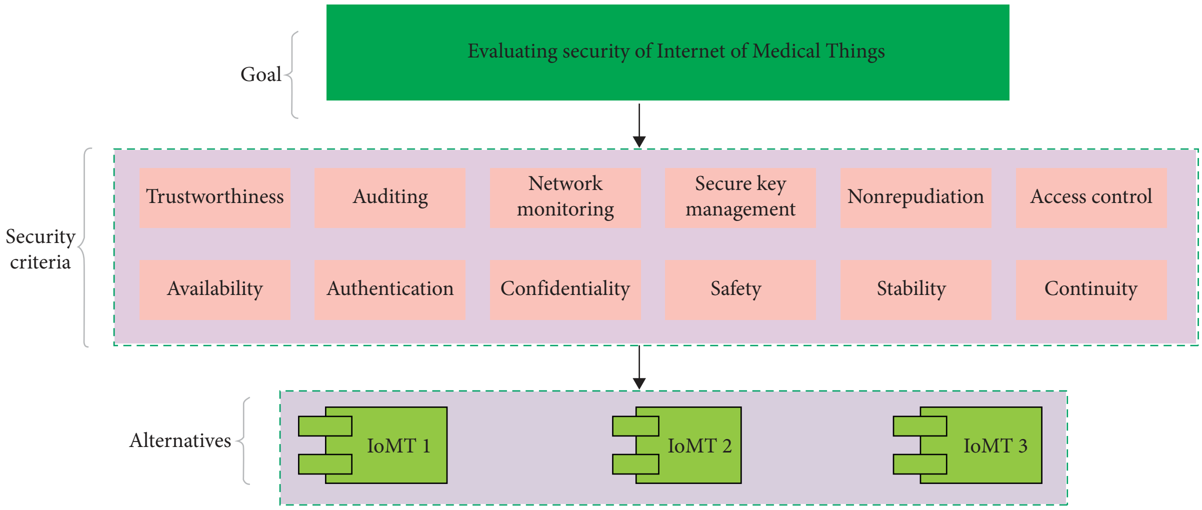
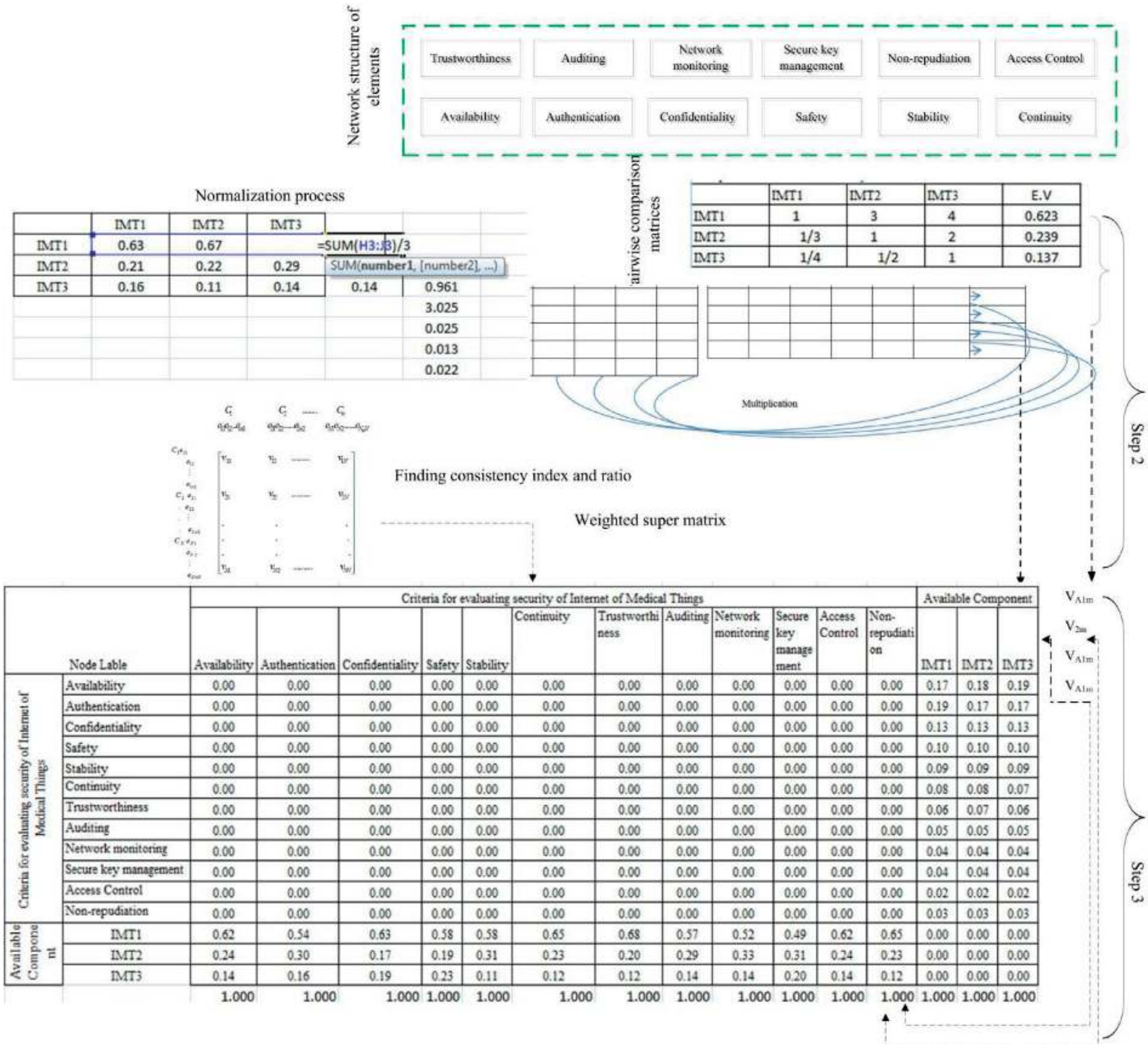


FIGURE 10: Goal, security criteria, and alternatives of the proposed research. The overall process of the proposed research is shown in Figure 11.



Normalization process

	IMT1	IMT2	IMT3		
IMT1	0.63	0.67		=SUM(H3:J3)/3	
IMT2	0.21	0.22	0.29	SUM(**number1**, [number2], ...)	
IMT3	0.16	0.11	0.14	0.14	0.961
					3.025
					0.025
					0.013
					0.022

	IMT1	IMT2	IMT3	E.V
IMT1	1	3	4	0.623
IMT2	1/3	1	2	0.239
IMT3	1/4	1/2	1	0.137

Weighted super matrix

		Criteria for evaluating security of Internet of Medical Things												Available Component		
	Node Lable	Availability	Authentication	Confidentiality	Safety	Stability	Continuity	Trustworthiness	Auditing	Network monitoring	Secure key management	Access Control	Non-repudiation	IMT1	IMT2	IMT3
Criteria for evaluating security of Internet of Medical Things	Availability	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.17	0.18	0.19
	Authentication	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.19	0.17	0.17
	Confidentiality	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.13	0.13	0.13
	Safety	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.10	0.10	0.10
	Stability	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.09	0.09	0.09
	Continuity	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.08	0.08	0.07
	Trustworthiness	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.07	0.06
	Auditing	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.05	0.05	0.05
	Network monitoring	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.04	0.04	0.04
	Secure key management	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.04	0.04	0.04
	Access Control	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.02	0.02	0.02
	Non-repudiation	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.03	0.03
Available Component	IMT1	0.62	0.54	0.63	0.58	0.58	0.65	0.68	0.57	0.52	0.49	0.62	0.65	0.00	0.00	0.00
	IMT2	0.24	0.30	0.17	0.19	0.31	0.23	0.20	0.29	0.33	0.31	0.24	0.23	0.00	0.00	0.00
	IMT3	0.14	0.16	0.19	0.23	0.11	0.12	0.12	0.14	0.14	0.20	0.14	0.12	0.00	0.00	0.00
		1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000

Figure 11: Process of the ANP for the proposed research.

Table 2: List of selected attribute.

Requirements	[7]	[8]	[9]	[10]	[11]	[12]	[31]	[32]	[33]	[34]	[35]	[36]	[37]	[38]	[39]	[40]	[41]	[42]
Confidentiality	*	*	*	*	*	*		*	*								*	
Authentication	*		*		*		*			*	*	*	*	*	*		*	*
Integrity	*	*	*	*	*	*		*			*	*						
Availability	*	*	*	*	*	*		*							*			
Authorization				*	*		*	*			*					*		
Physical security						*			*					*				
Continuity						*												
Trustworthiness	*				*													
Auditing	*																	
Network monitoring														*				
Secure key management			*											*				
Access control	*				*		*			*	*		*		*		*	*
Nonrepudiation					*	*		*			*							

Table 3: Comparison with respect to IoMT1.

	Availability	Authentication	Confidentiality	Safety	Stability	Continuity	Trustworthiness	Auditing	Network monitoring	Secure key management	Access control	Non-repudiation	EV
Availability	1	1/2	2	3	4	2	3	2	7	2	9	5	0.167
Authentication	2	1	2	4	3	3	2	5	3	5	7	2	0.189
Confidentiality	1/2	1/2	1	3	2	2	2	2	7	2	7	5	0.130
Safety	1/3	1/4	1/3	1	1/2	2	3	5	3	5	3	5	0.104
Stability	1/4	1/3	1/2	2	1	2	2	2	3	2	7	2	0.090
Continuity	1/2	1/3	1/2	1/2	1/2	1	3	3	2	2	3	5	0.082
Trustworthiness	1/3	1/2	1/2	1/3	1/2	1/3	1	2	3	2	4	3	0.064
Auditing	1/2	1/5	1/2	1/5	1/2	1/3	1/2	1	2	3	3	2	0.051
Network monitoring	1/7	1/3	1/7	1/3	1/3	1/2	1/3	1/2	1	2	2	2	0.036
Secure key management	1/2	1/5	1/2	1/5	1/2	1/2	1/2	1/3	1/2	1	2	2	0.038
Access control	1/9	1/7	1/7	1/3	1/7	1/3	1/4	1/3	1/2	1/2	1	2	0.022
Non-repudiation	1/5	1/2	1/5	1/5	1/2	1/5	1/3	1/2	1/2	1/2	1/2	1	0.028

CR = 0.985.

Table 4: Comparison with respect to IoMT2.

	Availability	Authentication	Confidentiality	Safety	Stability	Continuity	Trustworthiness	Auditing	Network monitoring	Secure key management	Access control	Non-repudiation	EV
Availability	1	3	2	2	4	2	3	2	7	2	5	2	0.179
Authentication	1/3	1	2	4	3	3	2	5	3	5	7	2	0.167
Confidentiality	1/2	1/2	1	3	2	2	2	2	7	2	7	5	0.132
Safety	1/2	1/4	1/3	1	1/2	2	3	2	3	5	3	5	0.099
Stability	1/4	1/3	1/2	2	1	2	2	2	3	2	7	2	0.092
Continuity	1/2	1/3	1/2	1/2	1/2	1	2	3	2	2	3	5	0.080
Trustworthiness	1/3	1/2	1/2	1/3	1/2	1/2	1	2	3	2	4	4	0.068
Auditing	1/2	1/5	1/2	1/2	1/2	1/3	1/2	1	2	3	3	2	0.055
Network monitoring	1/7	1/3	1/7	1/3	1/3	1/2	1/3	1/2	1	2	2	2	0.035
Secure key management	1/2	1/5	1/2	1/5	1/2	1/2	1/2	1/3	1/2	1	2	2	0.039
Access control	1/5	1/7	1/7	1/3	1/7	1/3	1/4	1/3	1/2	1/2	1	2	0.023
Non-repudiation	1/2	1/2	1/5	1/5	1/2	1/5	1/4	1/2	1/2	1/2	1/2	1	0.031

CR = 0.994.

Table 5: Comparison with respect to IoMT3.

	Availability	Authentication	Confidentiality	Safety	Stability	Continuity	Trustworthiness	Auditing	Network monitoring	Secure key management	Access control	Non-repudiation	EV
Availability	1	3	2	3	4	2	5	2	3	2	7	5	0.192
Authentication	1/3	1	2	4	3	5	2	5	3	5	7	2	0.173
Confidentiality	1/2	1/2	1	3	2	2	2	2	7	2	7	5	0.132
Safety	1/3	1/4	1/3	1	1/2	2	3	5	3	3	3	5	0.098
Stability	1/4	1/3	1/2	2	1	2	2	2	3	2	7	2	0.089
Continuity	1/2	1/5	1/2	1/2	1/2	1	3	3	2	2	3	2	0.073
Trustworthiness	1/5	1/2	1/2	1/3	1/2	1/3	1	2	3	2	2	3	0.059
Auditing	1/2	1/5	1/2	1/5	1/2	1/3	1/2	1	2	3	3	2	0.054
Network monitoring	1/3	1/3	1/7	1/3	1/3	1/2	1/3	1/2	1	2	2	2	0.039
Secure key management	1/2	1/5	1/2	1/3	1/2	1/2	1/2	1/3	1/2	1	2	2	0.040
Access control	1/7	1/7	1/7	1/3	1/7	1/3	1/2	1/3	1/2	1/2	1	2	0.023
Non-repudiation	1/5	1/2	1/5	1/5	1/2	1/2	1/3	1/2	1/2	1/2	1/2	1	0.028

CR = 0.10.

Table 6: For availability.

	IMT1	IMT2	IMT3	EV
IMT1	1	3	4	0.623
IMT2	1/3	1	2	0.239
IMT3	1/4	1/2	1	0.137

CR = 0.022.

Finally, the library of Springer was searched for the detail information in the area. Figure 8 shows the number of publications with the type of publications in the Springer library.

Figure 9 shows the article topic along with the total number of publications.

3. Applications of the Analytic Network Process for Evaluating Security of Internet of Medical Things

The analytic network process has several applications in different areas [11, 24, 27–29]. The reason behind using this method was to evaluate the security of IoMT, as this method works very well in situation where complexity exists. In the proposed research work, the analytic network process approach is used for security evaluation of Internet of Medical Things. The ANP method incorporates the criteria given for achieving the goal based on the available alternatives. This method helps in situation when complexity arises. The method adopted the ISO standard of security along with the identified security features from the literature. The ANP method consists of three parts: (a) the goal, (b) criteria, and (c) alternatives. Details regarding the ANP can be found in [30]; however, the following are the main steps:

(a) A particular phenomenon is to be divided into subparts

(b) A qualitative scale of measure is applied while this can be converted into a quantitative scale between 1 and 9

(c) The pairwise comparison is done for all the criteria along with alternatives

(d) The relative importance is found by finding the principal eigenvalue and the related eigenvector of the comparison matrix

(e) The consistency of matrix is measured

Priority vector "w" is calculated as follows:

$$A_w = \lambda_{\max} w. \tag{1}$$

$\lambda_{\max}$ is the major eigenvalue of the matrix "A," and "w" is its eigenvector. The value of "λ" is obtained by summing the column of the original matrix multiplied by the normalized EV. The principal EV is obtained by the sum of all "λ".

The "consistency index (CI)" and "consistency random (CR)" of the pairwise comparison matrix are computed by the following equation:

$$\begin{aligned} C_i &= \frac{\lambda_{\max} - n}{n - 1}, \\ CR &= \frac{CI}{RI}. \end{aligned} \tag{2}$$

The random consistency index (RI) table is given by Saaty and is shown in Table 1 [30].

(f) Construction of the supermatrix

(g) Conversion of the weighted supermatrix into the limit matrix for making the decision

(h) Deciding the most appropriate alternative from the limit matrix

Figure 10 shows the goal, criteria, and alternatives of the proposed research.

(i) Identification of attributes and scoring process: the process of identification of attributes was very tricky due to the reason that important attribute should be missed. For this purpose, the literature was searched and finally the attributes of the International Standard Organization (ISO) information security standard such as ISO/IEC 27000-series (ISO/IEC, 2018) along with 8 important attributes from the literature were identified. ISO/IEC 27000-series (ISO/IEC, 2018) is a well-known standard and widely accepted standard [12].

Table 2 shows the list of selected attributes.

After selecting the attributes for security evaluation, these attributes were shared with the experts in the field. The reason of sharing was to gather appropriate score for each component with respect to the defined attribute. Assigning the score to the relevant attribute was based on the expertise of the expert. Table 3 shows the comparison with respect to IoMT1.

Table 4 shows the comparison with respect to IoMT2.

Table 5 shows the comparison with respect to IoMT3.

Table 6 shows the comparison with respect to IoMT.

The rest of the calculations for the remaining attributes to IoMT were done the same as Table 6. After pairwise comparisons, all the calculations were brought together into the weighted supermatrix for the purpose to convert it into the limit matrix for decision-making about security evaluation. Table 7 shows the weighted supermatrix.

The weighted matrix was converted into the limit matrix by taking the power of the weighted matrix. This process was done till all the elements of each row become the same. The reason was to make decision based on the limit matrix. Table 8 shows the limit matrix.

Table 7: Weighted supermatrix.

Node label		Criteria for evaluating security of Internet of Medical Things												Available component		
		Availability	Authentication	Confidentiality	Safety	Stability	Continuity	Trustworthiness	Auditing	Network monitoring	Secure key management	Access control	Nonr-epudiation	IoMT1	IoMT2	IoMT3
Criteria for evaluating security of Internet of Medical Things	Availability	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.17	0.18	0.19
	Authentication	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.19	0.17	0.17
	Confidentiality	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.13	0.13	0.13
	Safety	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.10	0.10	0.10
	Stability	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.09	0.09	0.09
	Continuity	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.08	0.08	0.07
	Trustworthiness	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.07	0.06
	Auditing	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.05	0.05	0.05
	Network monitoring	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.04	0.04	0.04
	Secure key management	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.04	0.04	0.04
	Access control	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.02	0.02	0.02
	Non-repudiation	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.03	0.03
Available component	IoMT1	0.62	0.54	0.63	0.58	0.58	0.65	0.68	0.57	0.52	0.49	0.62	0.65	0.00	0.00	0.00
	IoMT2	0.24	0.30	0.17	0.19	0.31	0.23	0.20	0.29	0.33	0.31	0.24	0.23	0.00	0.00	0.00
	IoMT3	0.14	0.16	0.19	0.23	0.11	0.12	0.12	0.14	0.14	0.20	0.14	0.12	0.00	0.00	0.00

Table 8: Limit matrix.

Node label		Criteria for evaluating security of Internet of Medical Things												Available component		
		Availability	Authentication	Confidentiality	Safety	Stability	Continuity	Trustworthiness	Auditing	Network monitoring	Secure key management	Access control	Non-repudiation	IoMT1	IoMT2	IoMT3
Criteria for evaluating security of Internet of Medical Things	Availability	0.17	0.17	0.17	0.17	0.17	0.17	0.17	0.17	0.17	0.17	0.17	0.17	0.00	0.00	0.00
	Authentication	0.18	0.18	0.18	0.18	0.18	0.18	0.18	0.18	0.18	0.18	0.18	0.18	0.00	0.00	0.00
	Confidentiality	0.13	0.13	0.13	0.13	0.13	0.13	0.13	0.13	0.13	0.13	0.13	0.13	0.00	0.00	0.00
	Safety	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.10	0.00	0.00	0.00
	Stability	0.09	0.09	0.09	0.09	0.09	0.09	0.09	0.09	0.09	0.09	0.09	0.09	0.00	0.00	0.00
	Continuity	0.08	0.08	0.08	0.08	0.08	0.08	0.08	0.08	0.08	0.08	0.08	0.08	0.00	0.00	0.00
	Trustworthiness	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.00	0.00	0.00
	Auditing	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.00	0.00	0.00
	Network monitoring	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.00	0.00	0.00
	Secure key management	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.00	0.00	0.00
	Access control	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.00	0.00	0.00
	Non-repudiation	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.00	0.00	0.00
Available component	IoMT1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.60	0.60	0.60
	IoMT2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.25	0.25	0.25
	IoMT3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.16	0.16	0.16

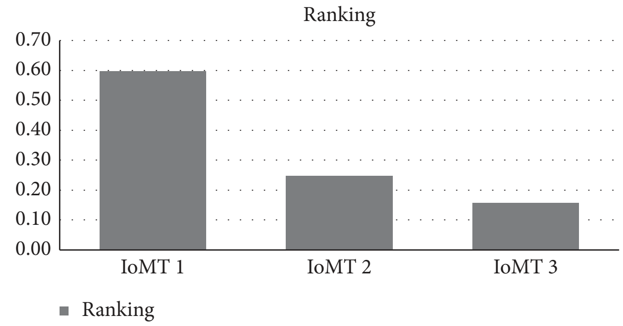


Figure 12: Ranking of IoMT.

Based on the limit matrix, we conclude that IoMT1 is the most secure component followed by IoMT2 and then IoMT3. Figure 12 shows the ranking of IoMT components.

4. Conclusion

The Internet of Medical Things is considered to be a significant part of healthcare which plays an important role. Communication among different devices such as smart sensors, wearable devices, handheld, and many other devices are connected in a network is possible due to the success of Internet of Things. For efficient and smooth running of healthcare, the security of different devices connected is mandatory. An efficient and robust security system is in dire need to cope with the attacks, threats, and vulnerability. The security evaluation of IoMT is an issue since the last few years. The proposed study is an endeavor toward the evaluation of the security of IoMT and using the analytic network process. The approach is applied using the ISO/IEC 27002 (ISO 27002) standard with the collection of some other important features from the literature. The results of the proposed research demonstrate the effective IoMT components which can further be used as secure IoMT.

Data Availability

No data were used to support the study.

Conflicts of Interest

The authors declare no conflicts of interest regarding this paper.

References

[1] X. Zhou, W. Liang, K. I.-K Wang, H. Wang, L. T. Yang, and Q. Jin, "Deep learning enhanced human activity recognition for internet of healthcare things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6429–6438, 2020.

[2] J. J. Kang, "Systematic analysis of security implementation for internet of health things in mobile health networks," in *Data Science in Cybersecurity and Cyberthreat Intelligence*, pp. 87–113, Springer, Cham, Switzerland, 2020.

[3] S. S. Rani, J. A. Alzubi, S. K. Lakshmanaprabu, D. Gupta, and R. Manikandan, "Optimal users based secure data transmission on the internet of healthcare things (IoHT) with lightweight block ciphers," *Multimedia Tools and Applications*, 2019.

[4] M. Asif-Ur-Rahman, F. Afsana, M. Mahmud et al., "Toward a heterogeneous mist, fog, and cloud-based framework for the internet of healthcare things," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4049–4062, 2019.

[5] J. J. P. C. Rodrigues, D. B. De Rezende Segundo, H. A. Junqueira et al., "Enabling technologies for the internet of health things," *IEEE Access*, vol. 6, pp. 13129–13141, 2018.

[6] A. M. Elmisery, S. Rho, and D. Botvich, "A fog based middleware for automated compliance with OECD privacy principles in internet of healthcare things," *IEEE Access*, vol. 4, pp. 8418–8441, 2016.

[7] S. Alam, M. M. R. Chowdhury, and J. Noll, "Interoperability of security-enabled internet of things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 567–586, 2011.

[8] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom workshops)*, pp. 618–623, Kona, HI, USA, March 2017.

[9] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," in *Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 336–341, Tokyo, Japan, December 2015.

[10] A. W. Atamli and A. Martin, "Threat-based security analysis for the internet of things," in *Proceedings of the International Workshop on Secure Internet of Things*, pp. 35–43, Wroclaw, Poland, September 2014.

[11] K. C. Park and D.-H. Shin, "Security assessment framework for IoT service," *Telecommunication Systems*, vol. 64, no. 1, pp. 193–209, 2017.

[12] R. Diesch, M. Pfaff, and H. Krcmar, "A comprehensive model of information security factors for decision-makers," *Computers & Security*, vol. 92, Article ID 101747, 2020.

[13] C. Hosmer, "IoT vulnerabilities," in *Defending IoT Infrastructures with the Raspberry Pi: Monitoring and Detecting Nefarious Behavior in Real Time*, pp. 1–15, Apress, Berkeley, CA, USA, 2018.

[14] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, 2017.

[15] W. Leister, M. Hamdi, H. Abie, and S. Poslad, "An evaluation framework for adaptive security for the iot in ehealth," *International Journal on Advances*, vol. 17, 2014.

[16] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "Sok: security evaluation of home-based iot deployments," in *Proceedings of the IEEE Symposium on Security and Privacy (SP)*, pp. 1362–1380, San Francisco, CA, USA, May 2019.

[17] A. Tekeoglu and A. Ş. Tosun, "An experimental framework for investigating security and privacy of IoT devices," in *Proceedings of the International Conference on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments*, pp. 63–83, Vancouver, BC, Canada, November 2017.

[18] M. Chernyshev and P. Hannay, *Security Assessment of IoT Devices: The Case of Two Smart TVs*, SRI Security Research Institute, Edith Cowan University, Perth, Australia, 2015.

[19] B. Ali and A. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *Sensors*, vol. 18, no. 3, p. 817, 2018.

[20] O. Mazhelis and P. Tyrväinen, "A framework for evaluating Internet-of-Things platforms: Application provider viewpoint," in *Proceedings of the IEEE World Forum on Internet of Things (WF-IoT)*, pp. 147–152, Seoul, Republic of Korea, March 2014.

[21] B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, "Security analysis of IoT devices by using mobile computing: A systematic literature review," *IEEE Access*, vol. 8, pp. 120331–120350, 2020.

[22] M. Li, S. Nazir, H. U. Khan, S. Shahzad, and R. Amin, "Modelling features-based birthmarks for security of end-to-end communication system," *Security and Communication Networks*, vol. 2020, pp. 1–9, Article ID 8852124, 2020.

[23] S. Nazir, S. Shahzad, S. Mahfooz, and M. N. Jan, "Fuzzy logic based decision support system for component security evaluation," *International Arab Journal of Information and Technology*, vol. 15, pp. 1–9, 2015.

[24] S. Nazir, S. Shahzad, M. Nazir, and H. U. Rehman, "Evaluating security of software components using analytic network process," in *Proceedings of the 11th International Conference on Frontiers of Information Technology (FIT)*, pp. 183–188, Islamabad, Pakistan, 2013.

[25] S. H. Almotiri, M. A. Khan, and M. A. Alghamdi, "Mobile health (m-health) system in the context of IoT," in *Proceedings of the IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pp. 39–42, Vienna, Austria, August 2016.

[26] Y. Karaca, M. Moonis, Y.-D. Zhang, and C. Gezgez, "Mobile cloud computing based stroke healthcare system," *International Journal of Information Management*, vol. 45, pp. 250–261, 2019.

[27] S. Nazir, S. Shahzad, Z. Hussain, M. Iqbal, and A. Keerio, "Evaluating student grades using analytic network process," *Sindh University Research Journal (Science Series)*, vol. 47, pp. 1–5, 2015.

[28] S. Nazir, S. Anwar, S. A. Khan et al., "Software component selection based on quality criteria using the analytic network process," *Abstract and Applied Analysis*, vol. 2014, pp. 1–12, 2014.

[29] S. Kheybari, F. M. Rezaie, and H. farazmand, "Analytic network process: An overview of applications," *Applied Mathematics and Computation*, vol. 367, Article ID 124780, 2020.

[30] T. L. Saaty, "Relative measurement and its generalization in decision making why pairwise comparisons are central in mathematics for the measurement of intangible factors the analytic hierarchy/network process," *Revista de la Real Academia de Ciencias Exactas, Fisicas y Naturales. Serie A. Matematicas*, vol. 102, no. 2, pp. 251–318, 2008.

[31] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018.

[32] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in *Proceedings of the IEEE World Congress on Services*, pp. 21–28, NewYork, NY, USA, June 2015.

[33] H.-J. Kim, H.-S. Chang, J.-J. Suh, and T.-S. Shon, "A study on device security in IoT convergence," in *Proceedings of the International Conference on Industrial Engineering, Management Science and Application (ICIMSA)*, pp. 1–4, Jeju Island, Republic of Korea, May 2016.

[34] L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville et al., "Internet of things in healthcare: Interoperatibility and security issues," in *Proceedings of the IEEE International Conference on Communications (ICC)*, pp. 6121–6125, Ottawa, Canada, June 2012.

[35] I. Alqassem and D. Svetinovic, "A taxonomy of security and privacy requirements for the Internet of Things (IoT)," in *Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management*, pp. 1244–1248, Selangor, Malaysia, December 2014.

[36] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pp. 417–423, San Jose CA, USA, November 2014.

[37] M. A. Razzaq, S. H. Gill, M. A. Qureshi, and S. Ullah, "Security issues in the Internet of Things (IoT): A comprehensive study," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 8, no. 6, pp. 383–388, 2017.

[38] C. Lee, L. Zappaterra, K. Choi, and H.-A. Choi, "Securing smart home: Technologies, security challenges, and security requirements," in *Proceedings of the IEEE Conference on Communications and Network Security*, pp. 67–72, San Francisco, CA, USA, October 2014.

[39] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed security model and threat taxonomy for the Internet of Things (IoT)," in *Proceedings of the International Conference on Network Security and Applications*, pp. 420–429, Taganrog, Rostov Region, Russia, July 2010.

[40] B.-C. Chifor, I. Bica, V.-V. Patriciu, and F. Pop, "A security authorization scheme for smart home internet of things devices," *Future Generation Computer Systems*, vol. 86, pp. 740–749, 2018.

[41] S. Hameed, F. I. Khan, and B. Hameed, "Understanding security requirements and challenges in Internet of Things (IoT): A review," *Journal of Computer Networks and Communications*, vol. 2019, Article ID 9629381, 14 pages, 2019.

[42] A. Hinduja and M. Pandey, "An ANP-GRA-based evaluation model for security features of IoT systems," in *Intelligent Communication, Control and Devices*, pp. 243–253, Springer, Berlin, Germany, 2020.