IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON LIGHTWEIGHT SECURITY AND PROVENANCE FOR INTERNET OF HEALTH THINGS

Received August 4, 2020, accepted August 13, 2020, date of publication August 17, 2020, date of current version August 28, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3017221

ISA Evaluation Framework for Security of Internet of Health Things System Using AHP-TOPSIS Methods

LANJING WANG[1,2], YASIR ALI[3], SHAH NAZIR[3], AND MAHMOOD NIAZI[4]

[1]Institute of Modern Logistics, Henan University, Kaifeng 475004, China
[2]School of Business, Henan University, Kaifeng 475004, China
[3]Department of Computer Science, University of Swabi, Swabi 23450, Pakistan
[4]Information and Computer Science Department, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia

Corresponding authors: Lanjing Wang (lanjing@henu.edu.cn) and Yasir Ali (Yasiuop007@gmail.com)

ABSTRACT Security has become a vital factor for any Internet of things network but it is of paramount importance for Internet of Health Things (IoHT). IoHT also known as Internet of Medical Things (IoMT) is integration of IoT and healthcare environment, where fragile data related to the patients is transmitted from IoT devices to server. During this transmission, if, any eavesdropping or intrusion occurs then it will not only lead to the serious mutilation of entire network but this data will be handled maliciously for wrong doings as well. Therefore, a proper security is indispensable for IoHT based equipments due to exposure to different attacks. Security of IoHT has been the burning issue in last couple of years. In this regard different security models, surveys, frameworks have been presented. In this article, a proposed Identified Security Attributes (ISA) framework is presented to evaluate the security features of IoHT based device in healthcare environment. The proposed framework uses hybrid MCDM methods such as Analytical Hierarchical Process (AHP) and Technique for Order Preference by Similarity to Ideal Solution (TOPSIS). This framework works in two phase: in first phase the weights of attributes are derived by using AHP method and in second phase security assessment of alternatives is performed based upon security criteria by using TOPSIS method. The outcomes of proposed security assessment framework demonstrate that the reliable and secure alternative among alternatives is selected in IoMT system. This approach can be used as a guideline for future use in IoMT systems or any other IoT based domain. To the best of our knowledge, it is novel approach to address the security assessment of IoT and these MCDM methods have never been used before for assessment and decision making in IoHT system for security.

INDEX TERMS Security, Internet of Things, AHP, IoHT, TOPSIS.

I. INTRODUCTION

Internet of health thing (IoHT) also knowna as Internet of Medical things (IoMT), is the network of healthcare devices connected to the cloud for sending and receiving data related to the chronical diseases of patients [1]. IoMT allows to reduce the unnecessary visits to hospital and alleviates burden on medical care system by providing connectivity over secure network between medical experts and patients; which, ultimately leads to saving of a lot of time and money [2], [3]. This is the reason, the number of IoT devices in healthcare network are increasing exponentially in last few years and contributed a lot towards the financial zone. According to Frost & Sullivan analysis report, IoMT market was worth $22.5 billion in 2016; this figure is expected to touch $72.02 billion in 2021 [2]. IoMT is sharply increasing such that 60% of global health care organizations have adapted it and by the end of 2020 it is estimated to increase by 27% [3].

IoT devices operating in healthcare environment are susceptible to various cyber threats and attacks.The healthcare industry faces 340% more security issues than any other industry and it's 200% more susceptible to data theft [3]. According to report over 90% of enterprises are facing at least on security breach [4]. Another study suggested that there is an average of 164 cyber threats detected per 1,000 connected host devices in IoMT system [5]. IoMT devices are deployed in network without considering the security in mind, this is the main reason that these devices suffer from confidentiality,

The associate editor coordinating the review of this manuscript and approving it for publication was Gautam Srivastava.

integrity and availability issues [6]. These vulnerabilities allow the cybercriminals to get access into the IoMT network and obtain the sensitive and personal data about the patients. One of the serious problems faced by IoMT devices is security and privacy issues. According to Jhonson and Jhonson IoMT devices like digital insulins are vulnerable to cyber threats [7]. In IoHT system, data relevant to patients is stored in the cloud and it is moving back and forth through millions of IoT devices and thus it spawns the vulnerability to data in their applications. Due to this vulnerability, many enterprises may not be willing to store IoT applications on the cloud. Therefore, risk assessment is mandatory prior to put their applications to the cloud and for mobile devices installing the IoT applications [8].

Sometimes, decision making regarding the selection of best security option for IoHT devices is an issue due to the many factors involved like evolving complex criteria pertaining to security, huge number of heterogeneous IoT devices, limited processing, and memory capabilities of these device. In light of these circumstances, lacking of proper security procedures and criteria is not a good approach. Keeping in view these factors, in this research work, we are presenting an evaluation framework in healthcare environment, which attempts to evaluate the IoT devices in light of security criteria and select the best IoT device as alternative among the list of devices. Security criteria or requirements are identified from literature review and International standard Organization (ISO) standard. A multi criteria is built in light of identified security requirements for decision making purposes. This selection criteria defines a full package of security, which can be implemented in any IoT devices in healthcare environment. A full-fledged secure IoHT system can be well described by fulfilling the security requirements or criteria such as confidentiality, integrity, availability, access control, authentication, authorization, network monitoring, physical security, network monitoring, secure key management, continuity, trustworthiness, auditing and non-repudiation. These requirements define the architecture of IoMT network in terms of considering different issues and challenges. The basic security requirements are defined in confidentiality integrity and availability (CIA model) [9], [10]–[13], [14]. The security of IoHT system has been addressed by different methods, but, in this regard, the multi criteria decision making (MCDM) approach is significant to mention. MCDM is also known as Multi Criteria Decision Analysis (MCDA) [15]. Multi criteria decision-making methods have various applications in different domains. Sometimes, it becomes very hard to find appropriate solution to the problems. Decision making is always a tough job due to imprecise, uncertainties and subjective nature of criteria [16].

For this purpose in this research work, we present ISA framework for security assessment and selection of IoHT based equipment with respect to identified security requirements or criteria in healthcare environment. These security requirements of IoT not only limited to specific application domain but they cover almost every area such as smart home, smart grid, smart agriculture, and smart city. The IoT security goals can be achieved by evaluating all the security requirements and implementing them for protecting IoT devices. In this research work, security of IoHT devices is assessed by using multi criteria decision making (MCDM) method and best option/equipment is to be selected from the alternatives.

The organization of the paper is as follows: section II describes motivation, in section III literature review has been discussed. In section IV, research method has been discussed, which includes criteria selection processes and proposed framework discussed along with and its validation by MCDM methods. Section V ends with conclusion.

II. CONTRIBUTION AND RESEARCH GAP

The contributions made by earlier methods for security evaluation in IoHT system are great but still there exists some drawbacks and gaps that are required to be addressed:

- Criteria identified by previous studies are not sufficient enough to meet the all security requirements of IoT. Therefore, for security assessment a complete pack of security requirements needs to be considered. This work has targeted the same to include all the security requirements in order to provide full-fledge IoT security solution in healthcare environment. Criteria like continuity, trustworthiness, network monitoring and secure key management were neglected by previous works.
- In previous works, the security requirements are collected only from the literature but in this work, we integrated both literature and ISO security standard ISO/IEC 27000-series (ISO/IEC, 2018), which is well-known security standard for implementing security all over the world.
- In this work, two MCDM methods such as AHP and TOPSIS have been used, which are ideal to provide a good platform for assessment and decision making. AHP requires less quantitative data and in TOPSIS information loss is less in the evaluation processes.
- To the best of our knowledge, this is novel approach, which combines both AHP-TOPSIS for security assessment in and decision making purposes in healthcare environment

III. MOTIVATION

The proposed research work is motivated to achieve the following objectives.

- Decision making in IoHT is big challenge due the number of criteria and sub-criteria involved. The prime focus of this research work is to select the best security solutions for IoHT systems by using hybrid MCDM approach
- The security of IoMT system is getting a burning topic in last decade so this motivation led us to assess the security of IoMT based system
- There exists a research gap between existing work and proposed work. This proposed work is based upon

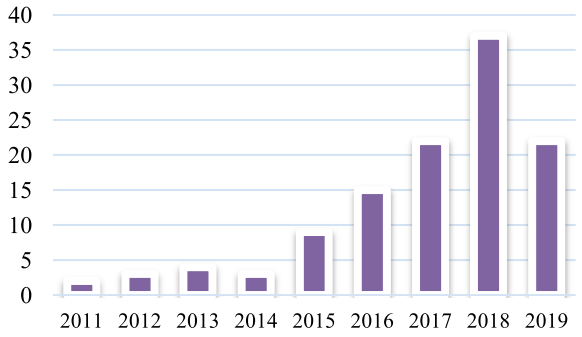


FIGURE 1. Research trend in IoT security.

security requirements identified from both sources such as ISO security standard and literature. ISO standard for security requirements have never been used before for security evaluation or assessment criteria

IV. RELATED WORK

IoT devices have limited processing, bandwidth and memory capabilities due to their limited structures, which make them vulnerable to many security threats and attacks [17], [18]–[20]. This is the main reason, that IoT security has been the most intriguing and busy research area since last decade i.e. 2011 to 2019 as shown in Fig 1. To address the security and privacy issues in IoT different frameworks have been presented like [21]–[26]. IoT devices experience more serious privacy security risks [27]. Especially, in healthcare environment these risks become more serious and sever due the nature of data handled by the network. As, data related to patients are stored in cloud server of hospital center, required to be kept secured [28].

For security of IoMT or IoHT many works are available but in this literature study, we are restricting our discussion to MCDM methods such as AHP and TOPSIS. But, still, some frameworks for security in IoMT are discussed like Leister *et al.* [29] presented evaluation framework for adaptive security in IoHT. Nkomo and Brown [30] presented a hybrid cybersecurity framework for IoMT. Jan *et al.* [31] presented the authentication of nodes for streaming of data. Similarly, there are many other frameworks intended to address the security of IoMT system are presented [32]–[38].

MCDM methods have wide range of applications in IoMT system. The role of multi criteria decision making analysis in healthcare has been briefly discussed by Frazão *et al.* [39]. These methods not only address the security issues but are also applied for variety of the purposes like assessment and selection in IoMT. Drake *et al.* [40] used MCDM methods for contracts and tender process in healthcare environment. Liu *et al.* [41] presented a hybrid MCDM model for mobile healthcare system.

We highlighted those related work, which addressed the security of IoT in healthcare by using multi criteria decision making methods such as AHP and TOPSIS or both together.The detail of AHP or TOPSIS method or both for security assessment and decision making in IoMT based systems are given in Table 1.

All frameworks, models and schemes for providing security solutions towards IoMT using MCDM methods like AHP, TOPSIS or any other MCDM methods are reported along with the features or criteria. The summary of our literature is depicted in Table 2.

V. RESEARCH METHOD

The security of IoHT devices is indispensable due to ubiquitous and multi sensor approach adapted by IoHT network. In this research, our prime focus is to present proposed ISA framework to provide solution towards the security challenges faced by IoMT system. The proposed security framework of security evaluation and selection of IoHT devices based upon identified set of attributes as depicted in Figure 1. The main idea is before introducing an IoT device into operating environment such as healthcare environment, it is necessary to check its security with respect to security criteria. In this research, both MCDM methods such AHP and TOPSIS have been used for assessment and selection of IoHT device with respect to security features. Research method has the following subsections: In first section, security requirements or criteria are identified, in second section, proposed framework is presented, in third section weights are assigned to criteria by using AHP and fourth section describes how TOPSIS method has been used for assessment and decision making.

A. SELECTION OF SECURITY REQUIREMENTS OR CRITERIA

The security requirements also known criteria are identified and selected for the security evaluation of IoT devices in healthcare environment. These security requirements not only limited to specific application domain but they cover almost every application domains such as smart health, smart home, smart grid, smart agriculture, smart city etc. The security goal of IoHT can be achieved by evaluating all the security requirements and implementing them for protecting the IoT devices in healthcare environment. In this research work, security requirements are identified from both sources such as literature and International Standard Organization (ISO) information security standard such as ISO/IEC 27000-series (ISO/IEC, 2018). ISO/IEC 27000-series (ISO/IEC, 2018) is a well-known standard and widely accepted standard [14]. This standard implements an information security management system based upon defined set of basic requirements. This is also current standard in Australia. This standard, provides guidance pertaining to controlling, implementation, managing measures and approach towards risk management [14]. Similarly, after studying literature, many security requirements or criteria from various research articles are collected and detail about these is given in Table 3. In this research work, 8 security requirements from literature and 5 attributes are derived from ISO/IEC 27000 (2018) standard. Finally,

TABLE 1. AHP and TOPSIS Methods for security assessment in IoMT/healthcare.

Ref & Author	MCDM method	Year	Description
Alsubaei et al [42]	AHP	2019	This framework known as IoMT-SAF, uses AHP for assigning degrees to the IoMT solutions by keeping components level and holistic security in mind
Liao et al [43]	AHP	2016	This method uses AHP to assess the cloud services in healthcare environment in order to provide cost effectiveness and quality
Alsubaei et al [44]	AHP	2018	This framework uses AHP for ranking solutions in IoMT enviroment based on assessment criteria by using security features
Rajasekaran et al [45]	AHP	2019	Although, this model does not address the security of IoMT but the core focus is upon the energy distribution among the nodes in IoMT network
Kumar et al [46]	Fuzzy AHP-TOPSIS	2020	This method uses fuzzy AHP-TOPSIS method for assessment of harmful factors affecting the security break in medical care system
Dimitrioglou et al [47]	AHP	2017	It uses AHP model to evaluate the IoT based applications or services for dementia care. AHP method is used for decision making and this work has not addressed the security
Al-Zahrani et al [48]	TOPSIS and other MCDM methods	2020	This work attempts to evaluate the security of software in healthcare environment
Rajak et al [49]	AHP and Fuzzy TOPSIS	2019	A model is presented to evaluate and selection the best mobile health (M-health) application based upon identified factors
Büyüközkan et al [50]	Fuzzy AHP & TOPSIS	2012	Proposed method provides quality assessment of quality services delivered to the customer via internet
Rađenović et al [51]	AHP-TOPSIS	2017	This evaluation model attempts to evaluate three softwares performances used in electronic healthcare.

total of 13 security requirements are selected based upon their impact on IoMT security, frequency of occurrence and factor of commonality in literature. Selected security attributes along with sources are marked in Table 4. The overall picture of steps taken towards the completion of research work in summarised fashion is depicted in Fig 2.

Frequency of attributes citation based on number of papers in literature is depicted in Fig 3.

The overall procedure for selection of security requirements consists of different steps: in step one 119 attributes are identified from literature, in second step duplicates or repetition of attributes is removed, in third step attributes are identified from ISO standard, in 4^{th} step all attributes are combined and in last step final attributes for security assessment have been selected. Procedure for selection of security attributes/criteria is shown in Fig 4.

All finally selected attributes for security assessment in this research work have been explained in Table 5.

In this research work, four IoT based equipments or devices are selected as alternatives for decision making. These alternatives are labelled as D_1 D_2, D_3 and D_4. The hierarchical structure of 13 security requirements for "n" number of alternatives or IoHT devices is depicted in Fig 5.

B. PROPOSED FRAME WORK FOR SECURITY EVALUATION AND DECISION MAKING

The proposed framework for security evaluation is also known as Identified Security Attributes (ISA) framework. The main objective of framework is to achieve the security evaluation of IoT devices or alternatives based upon the identified security criteria in healthcare environment. After identifying and selection of security requirement or attributes, the IoT devices as alternative are selected and data is collected from by consulting the security experts in the field of IoT security. Our data collection technique inspired by Delphi method [68]. The proposed security framework for evaluation and decision making about security of IoT devices in medical care system is shown in Fig 6. This framework works in two phases: in first phase AHP method assigns weights and in second phase TOPSIS method has been used for ranking of alternatives.

C. ASSIGNING WEIGHTS TO SECURITY REQUIREMENTS OR CRITERIA BY USING AHP

In this research Analytic Hierarchy Process (AHP) method has been used for assigning weights to the criteria. This method is ideal for problem situations that involve multi-criteria decision making situations. There are many reasons for selecting this method like, it focuses upon diminishing the cognitive errors by simplifying, partitioning, and comparing multiple attributes. It is not only suitable for comparing qualitative indices but also for quantitative indices. Thus, it has various applications in domains like selection, assessment, resource allocation, conflicts resolution, priority and ranking, and optimization. AHP method is subjective in nature, it means the experts or decision makers assign weights

TABLE 2. Summary of literature study.

Ref	MCDM used? If yes, then which one.	Security addressed?	No of attributes	Attributes source	Attributes Detail/Criteria
[52]	ANP-GRA	Yes	12	Literature	▪ Authentication ▪ Privacy protection ▪ Anti DDOS ▪ Secure Cloud computing ▪ Encryption mechanism ▪ Node information certificate ▪ Platform security ▪ Anti-attack security ▪ Information application security ▪ Secure multi-party computation ▪ Application risk of IPV6 ▪ Heterogeneous network recognition
[42]	AHP	Yes	16	IoMT scenario & stakeholders	▪ Access control ▪ Authentication ▪ Cloud service isolation ▪ Incident response ▪ Intrusion prevention ▪ Memory protection ▪ Physical security ▪ Privacy ▪ Regulatory compliance ▪ Secure Root-of-Trust ▪ Secure connectivity ▪ Secure data storage ▪ Secure development life cycle ▪ Secure update ▪ Software security ▪ Web Security
[43]	AHP	Somehow	14	Not specified	▪ Convenient software ▪ Software scalability ▪ Cloud-based medical image exchange Integration of information and health care services Cloud service delivery ▪ Data storage security ▪ System stability ▪ Software research and development ▪ Testing and debugging ▪ Cloud management issues Flexible and expandable framework ▪ Convenient information sharing ▪ Cost-effectiveness ▪ Regulatory compliance
[29]	NO	Yes	N/A	N/A	N/A
[30]	NO	Yes	03	N/A	▪ Confidentiality ▪ Integrity ▪ Availability
[31]	NO	YES	N/A	N/A	N/A
[40]	MCDA	No	04	N/A	▪ Innovation ▪ Economic impact ▪ Equity ▪ Other
[32]	NO	YES	N/A	N/A	N/A
[41]	DEMATEL+ DANP +Modified VIKOR	NO	03	Literature	▪ Technological dimension ▪ Environmental dimension ▪ Subjective dimension
[45]	AHP	No	07	Literature	▪ Energy for transmission ▪ Energy for sampling ▪ CPU energy consumption ▪ Energy for reception ▪ Energy for memory access ▪ Energy for initialization ▪ Energy for sensor module

TABLE 2. ***(Continued.)*** **Summary of literature study.**

[46]	Fuzzy AHP & TOPSIS	Somehow	06	Literature	▪ Social Engineering ▪ Ransomware ▪ Human Error ▪ Outdated IT Infrastructure ▪ Low access control management ▪ Medjacking
[47]	AHP	No	03	Literature	▪ Effectiveness ▪ Safety ▪ Patient perspective
[48]	TOPSIS & Fuzzy ANP	Somehow	04	Literature	▪ Confidentiality ▪ Integrity ▪ Availability ▪ Satisfaction
[49]	AHP and fuzzy TOPSIS	No	09	Literature	▪ User satisfaction ▪ Compatibility ▪ Functionality ▪ Security ▪ Accessibility ▪ Easy to learn and use ▪ Empathy ▪ Information Quality ▪ Responsiveness
[34]	No	Yes	N/A	N/A	N/A
[35]	No	Yes	04	Literature	▪ Security ▪ Privacy ▪ Key size ▪ Multi-level security
[36]	No	Yes	05	Performance evaluation metrics	▪ Accuracy ▪ Precision ▪ Recall ▪ F1-score ▪ False positive rate (FPR)
[37]	No	Somehow	N/A	N/A	N/A
[38]	No	Yes	N/A	N/A	N/A
[50]	Fuzzy AHP & TOPSIS	No	06	Literature	▪ Tangibles ▪ Responsiveness ▪ Reliability ▪ Information quality ▪ Assurance ▪ Empathy
[51]	AHP-TOPSIS	No	06	N/A	▪ Number of users ▪ Data redundancy ▪ Monthly increase of interoperability rates ▪ Rate of return ▪ Monthly increase of the utilisation of data ▪ Compliance with HIPPA principles
[44]	AHP	Yes	12	Open Web Application Security Project (OWASP), the International Organizations of Standardizatio n (ISO)	▪ Secure administration ▪ Strong authentication ▪ Secure updates ▪ Intrusion prevention ▪ Protected memory ▪ Secure communications ▪ Secure web interface ▪ Secure hardware ▪ Secure software ▪ Secure storage ▪ Regulatory compliance ▪ Secure root of trust
Proposed work	AHP-TOPSIS	Yes	13	Literature and International Standard organization ISO/IEC 27000-series (ISO/IEC, 2018)	▪ Confidentiality ▪ Authentication ▪ Integrity ▪ Availability ▪ Authorization ▪ Physical Security ▪ Continuity ▪ Trustworthiness ▪ Auditing ▪ Network monitoring ▪ Secure key management ▪ Access Control ▪ Non-repudiation

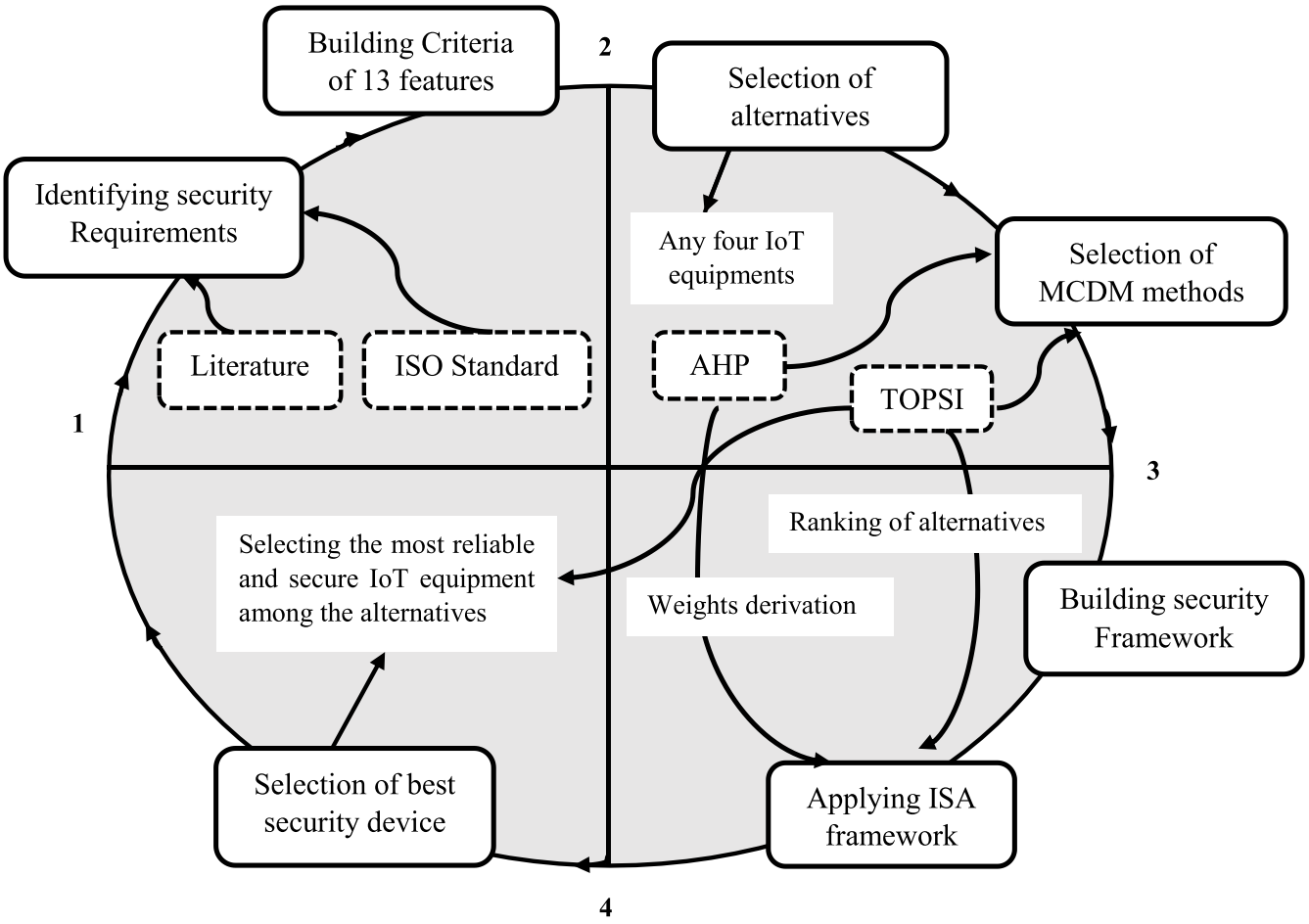


FIGURE 2. Flow of research work.

TABLE 3. List of all security requirements collected from literature and ISO standard.

Citation	Security Features											
[9]	Confidentiality	Integrity	Availability	Authentication	Authorization	Access Control	Trustworthiness	Auditing				
[53]	End to End security			Authentication	Authorization	Access control						
[54]	Anonymity	Integrity	Availability	Non-repudiation	Authorization	Access control	Resiliency	Self-organization	Information Protection	Exception Handling		
[55]	Lightweight Protocol	Cryptography	Data protection	Communication Security	Physical protection	Identification	Permission					
[56]	Attack resilience	Client Privacy		Authentication		Access Control						
[57]	Non Repudiation	Integrity	Contextual integrity	Authentication	Authorization	Access Control	Intrusion Detection					
[58]	Tracking	Integrity	Mutual trust	Authentication	Privacy	Digital forgetting						
[10]	Confidentiality	Integrity	Availability									
[59]	Resilience to attack	Client Privacy		Authentication		Access Control						
[60]	User authentication	Device authentication	Network Monitoring	Secure key management	Physical protection							
[11]	Confidentiality	Integrity	Availability	Authentication	Light weight algorithm	Heterogeneity	Policies	Key Management				
[12]	Confidentiality	Integrity	Availability		Authorization	Identification						
[61]	Resilience to attack	Client privacy	User identification	Data authentication	Secure storage	Access control	Identity management	Secure data communication	Availability	Secure N/W Access	Secure content	Temper resistance	Secure Environment Execution
[62]	Theft resistance	Authorization	Cloud federated authentication									
[13]	Confidentiality	Integrity	Availability	Authentication	Authorization	Trust	Auditing	Access control	Non repudiation	Privacy	Anonymity	Reply protection	Resilience to attacks
[63]	Privacy	Confidentiality	Secure routing	R.R management	Attack detection							
[52]	Authentication	User access control	Key agreement	Privacy protection	Encryption	Anti DDOS	Privacy	Platform protection				
[14]	Confidentiality	Availability	Integrity	Non repudiation	Continuity	Physical Security						

TABLE 4. Final list of selected security requirements along with sources.

	Literature																	
Requirements	**[9]**	**[53]**	**[54]**	**[55]**	**[56]**	**[57]**	**[58]**	**[10]**	**[59]**	**[60]**	**[11]**	**[12]**	**[61]**	**[62]**	**[13]**	**[63]**	**[52]**	**[14]**
Confidentiality	√		√	√				√			√	√			√	√		√
Authentication	√	√			√	√	√		√	√	√		√		√	√	√	
Integrity	√		√			√	√	√			√	√			√			√
Availability	√		√					√			√	√	√		√			√
Authorization		√	√			√						√		√	√			
Physical Security				√						√								√
Continuity																		√
Trustworthiness	√														√			
Auditing	√																	
Network monitoring										√								
Secure key management										√	√							
Access Control	√	√			√	√			√				√		√	√	√	
Non-repudiation			√			√									√			√

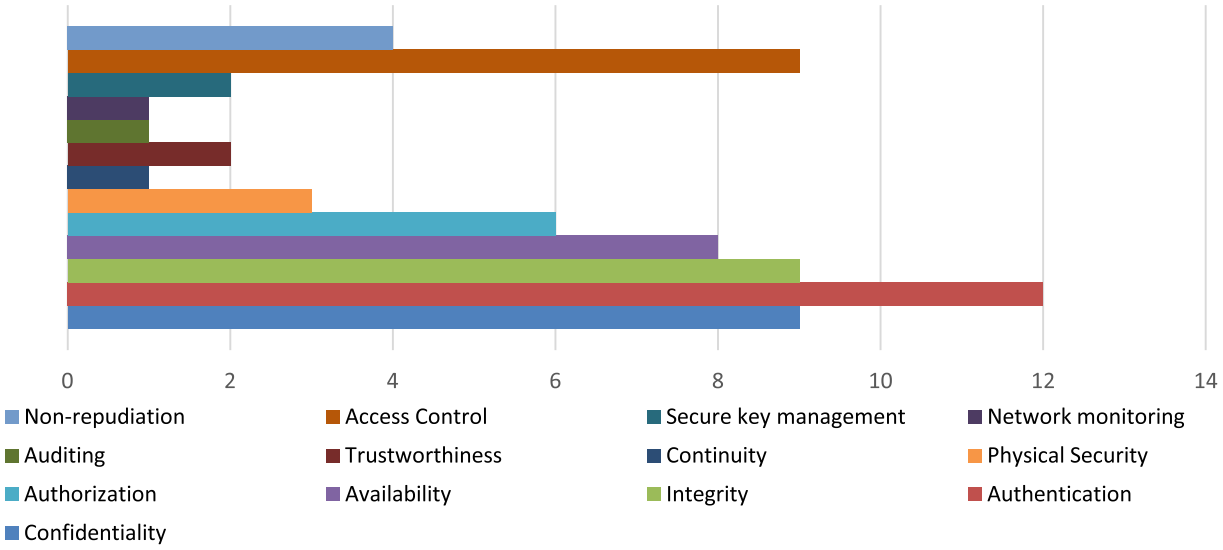


FIGURE 3. Frequency of attributes citation in literature.

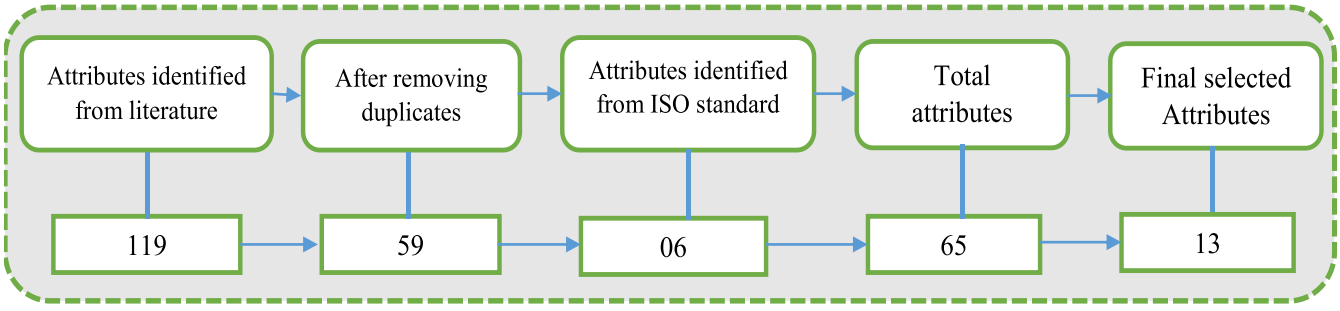


FIGURE 4. Procedure of selection security requirements.

TABLE 5. Attributes detail.

Ref#	Attribute	Description
[64]	Confidentiality	It means protecting user privacy and concealing data from unauthorized entity or user
[64]	Authentication	Process of verifying and differentiating the identities that access the entities
[14]	Access control	Access to assets is authorized and restricted based on business and security requirements
[14]	Continuity	Ability to continuously deliver the intended outcome despite adverse cyber events
[9]	Auditing	A log will keep all detail of services, request to services, request made by whom and when
[9]	Trustworthiness	Any untrusted and malicious data can come from trusted node or sensor
[60]	Network monitoring	The procedure of detecting and reporting in IoT based network about intrusion and DOS attacks
[65] [66]	Physical security	Physical security is to deny the physical access or damage to the IoT devices It can be accessing the USB or physical ports or bypassing configuration or permissions
[65]	Non-repudiation	According to this property the any two IoT entities must not the deny the transfer of message between them
[65]	Integrity	It ensures that sensitive data must not be altered and destroyed and must be protected in correct, reliable and complete form
[64] [67]	Authorization	Only the authorized devices and the users get access to the network services or resources or procedure of allowing, denying, and restricting access to entities
[64, 65]	Availability	Data and services of IoT devices accessible and usable for authorized users only. It can be affected by natural disasters like earthquake, flooding and storm or it can be affected by human accidental or deliberate activities The most famous mechanisms to protect availability are: firewall, IDS, and redundancy methods
[11, 60]	Secure key management	IoT devices to exchange data with trust and confidentiality among the IoT nodes and sensors

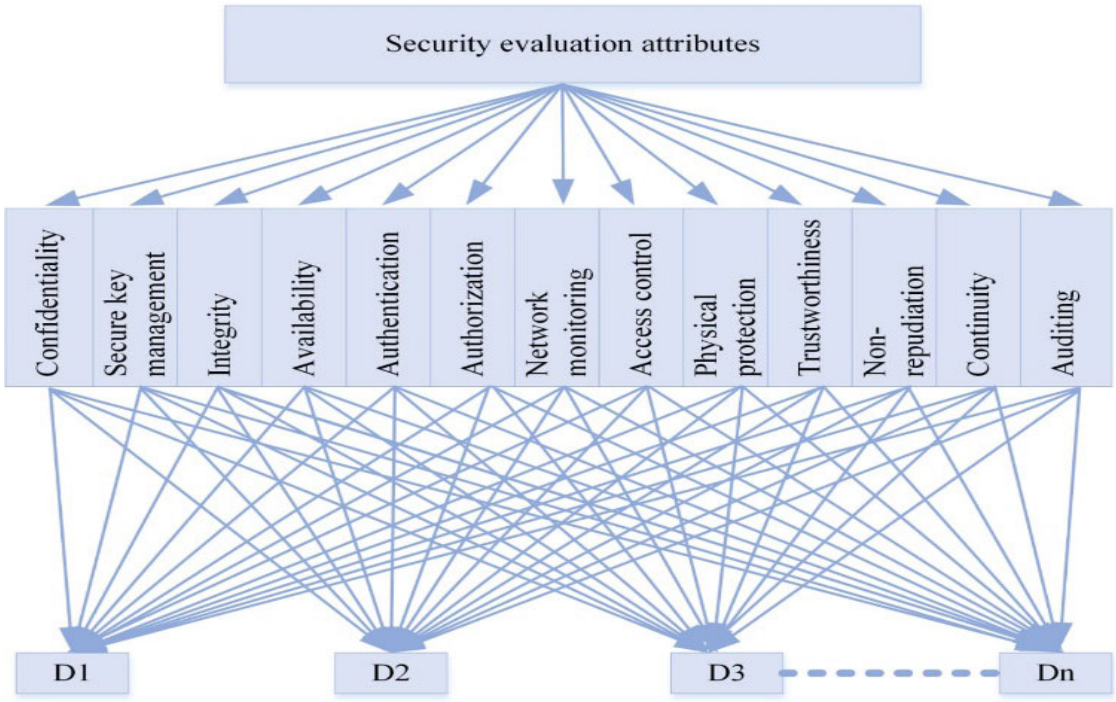


FIGURE 5. Hierarchical structure of alternatives and criteria.

based upon their opinions [69]. AHP is a technique which prioritizes each alternative based upon their significance of hierarchy or goals identification [70]. According to [71]–[73] the AHP method involves the following steps.

Step-1. Identification of criteria and alternatives

In first step criteria, sub-criteria and alternatives are identified and they are represented in the form of hierarchical shape.

TABLE 6. Criteria, alternatives and codes.

Criteria	Codes	Criteria	Codes
Confidentiality	C_1	Network Monitoring	C_8
Integrity	C_2	Authentication	C_9
Availability	C_3	Auditing	C_{10}
Access control	C_4	Authorization	C_{11}
Physical security	C_5	Continuity	C_{12}
Non Repudiation	C_6	Secure Key management	C_{13}
Trustworthiness	C_7		
Alternatives	**D_1, D_2, D_3, D_4**		

Step-2. Assigning weights or scores

In this step, weights are assigned by experts based upon the relative importance of each criteria based upon a defined scale. The qualitative scores are converted into quantitative form.

Step-3. Building a pairwise comparison matrix

A pairwise matrix is obtained by using a scale from 1 to 9. In comparison matrix a_{ij} shows the significance of i^{th} criteria relative to j^{th} criteria. If a_{ij} is greater than one then the i^{th} criterion is more important as compared to j^{th} criterion and when a_{ij} is less than one the i^{th} criterion is less important. For $a_{ij} = 1$, it means both are having same importance. In this comparison is done in the form of matrix as shown in equation (1).

$$A = \begin{bmatrix} 1 & a_{12} \cdots & a_{1n} \\ \frac{1}{a_{12}} & 1 \cdots & a_{2n} \\ \vdots & \vdots & \vdots \\ \frac{1}{a_{1n}} & \frac{1}{a_{2n}} & 1 \end{bmatrix} (1) \quad (1)$$

Step-4. Constructing a normalized pairwise comparison matrix

In this step, the sum of columns of matrix is calculated, each element is divided by sum of column and then averages of rows are calculated in normalized pairwise comparison matrix. In this steps weights of criteria are calculated, which show the priorities of each criterion. Weights are determined by two methods i.e. Lambda max (λ_{max}) and geometric mean in AHP. λ_{max} is eigenvalue and equation for finding λ_{max} is given as.

$$\lambda_{max} = \frac{1}{n} \sum_{i=1}^{n} \frac{(Aw)_i}{w_i} \quad (2)$$

Step-5. Consistency matrix

Consistency matrix is built to check whether the comparison is consistent or not. In this step Consistency Index (C.I) is found by using equation (3) and Consistency Ratio (C.R) is calculated by equation (4). In this step the each element of first column in pairwise comparison matrix is multiplied with the weights of first row in normalized pairwise matrix, similarly this procedure is repeated for all the columns.

$$C.I = \frac{\lambda_{max} - n}{n - 1} \quad (3)$$

$$C.R = \frac{C.I}{R.I} \quad (4)$$

TABLE 7. AHP pairwise comparison scale.

Linguistic Term	Scale
Extremely preferred	9
Very strongly to extremely	8
Very strongly preferred	7
Strongly to very strongly	6
Strongly preferred	5
Moderately to strongly	4
Moderately preferred	3
Equally to moderately	2
Equally preferred	1

If, CR value is 0.1 or less than 0.1 then it acceptable, otherwise the procedure will be repeated from the beginning.

D. AHP NUMERICAL WORK

In first step of AHP, a decision matrix was built by using a set of identified requirements or criteria and alternatives. A questionnaire is presented to the different experts in field of IoT security and some questions related to four IoT alternatives against the identified set of attributes were asked. Like, which security attribute is important and how much they are related to each other. Data from different experts panel pertaining to each IoMT security criterion is reported and prioritized based upon numerical weightage for different IoHT alternatives. The identified security requirements are labelled as $\boldsymbol{C_1}$, $\boldsymbol{C_2}$, $\boldsymbol{C_3}$, $\boldsymbol{C_4}$, $\boldsymbol{C_5}$, $\boldsymbol{C_6}$, $\boldsymbol{C_7}$, $\boldsymbol{C_8}$, $\boldsymbol{C_9}$, $\boldsymbol{C_{10}}$, $\boldsymbol{C_{11}}$, $\boldsymbol{C_{12}}$ and $\mathbf{C_{13}}$. Similarly, the alternatives are coded as $\boldsymbol{D_1}$, $\boldsymbol{D_2}$, $\boldsymbol{D_3}$, and $\boldsymbol{D_4}$ as shown in Table 6. These codes are only assigned for simplicity in calculation.

A comparison matrix is made based upon comparing criteria by following pairwise comparison scale [16]. AHP pairwise comparison scale is shown in Table 7. In this table, highest score is 9, it means a security attribute having 9 value is extremely important as compared to other security attribute(s) and lowest score is 1, which means equally preferred in comparison with other attributes. Like C_9 is equally important as C_1, C_2, C_3 as shown in pairwise comparison matrix. Similarly, a criterion is equally important, when it is compared with itself so the values in this case are 1. All the values in diagonal show equal importance.

A pairwise comparison matrix, is built of all security attributes by using equation (1) based upon AHP pairwise comparison scale. Criteria weights are calculated with nor-

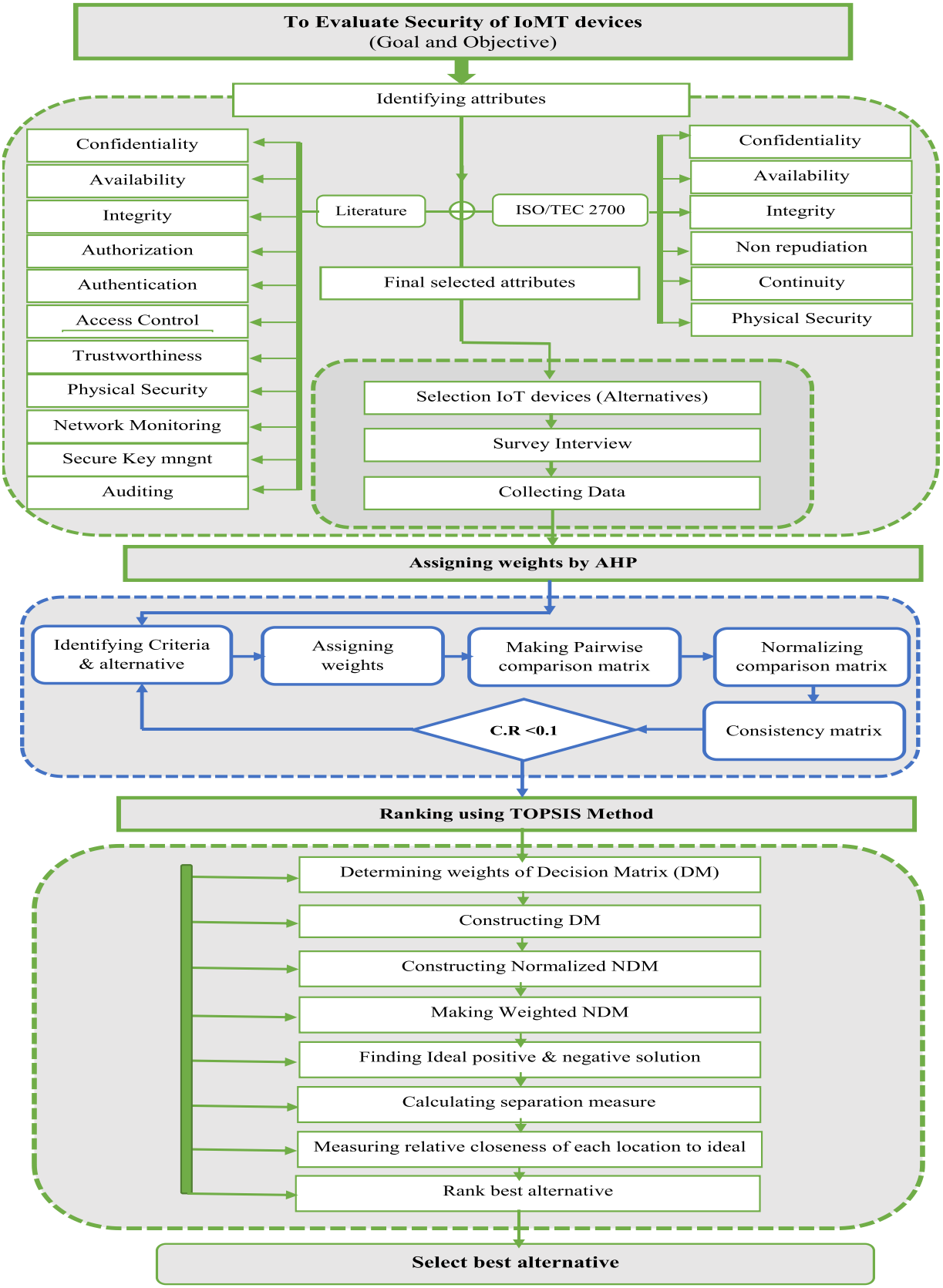


FIGURE 6. Proposed ISA framework for security evaluation and decision making.

TABLE 8. Criteria weights.

Criteria	Weights	Criteria	Weights
C_1	0.15	C_8	0.06
C_2	0.12	C_9	0.07
C_3	0.14	C_{10}	0.03
C_4	0.11	C_{11}	0.03
C_5	0.11	C_{12}	0.02
C_6	0.07	C_{13}	0.02
C_7	0.07		

malized pairwise comparison matrix by using equation (2) and results are depicted in Table 8. The criteria weights are numbers, which show the importance of each criterion. C_1 is given more weight or score among the criteria listed in Table 8, it means it is very important criteria as suggested by the experts' panel. Similarly, C_{12} and C_{13} both criteria are having lowest values among others, it means that these are not important criteria as other criteria are important.

The calculated criteria weights are further verified by consistency ratio (C.R) value and the procedure of verification is continued by finding the Lambda max. By using equation (2), Lambda max (λ_{max}) can be calculated as follows.

$$\lambda_{\max} = \frac{1}{13}\left[\frac{2.27}{0.15}+\frac{1.96}{0.12}+\frac{2.13}{0.14}+\frac{1.72}{0.11}+\frac{1.82}{0.11}+\frac{1.06}{0.07}+\frac{1.03}{0.07}+\frac{0.86}{0.06}+\frac{0.88}{0.07}+\frac{0.48}{0.03}+\frac{0.47}{0.03}+\frac{0.31}{0.02}+\frac{0.23}{0.02}\right]$$

$$\lambda_{\max} = \frac{1}{13}[15.528 + 16.029 + 15.689 + 15.067 + 16.027 + 15.497 + 14.802 + 15.045 + 13.409 + 13.866 + 13.793 + 13.817 + 14.393]$$

$$\lambda_{\max} = \frac{1}{13}[192.96]$$

$$\lambda_{\max} = 14.8$$

The Random Index (R.I) for "N" number of criteria is shown in Table 9 [74]. In this research work, we have used 13 security requirements as the number of criteria, so the value of R.I is 1.56 according to Table 9.

Consistency index is calculated by using equation (3) as given as below.

$$\text{C.I} = \frac{14.8 - 13}{13 - 1} = 0.15$$

Consistency Ratio (C.R) is calculated by using equation (4) below as.

$$\text{C.R} = \frac{0.15}{1.56} = 0.96 < 0.1 \text{ or } (9.6\% < 10\%)$$

As, the value of C.R is less than 0.1 or 10 %, it means that inconsistency is reliable and we can proceed towards further security evaluation.

Pairwise comparison matrix

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}
C_1	1	1	1	3	2	5	2	5	1	5	3	5	5
C_2	1	1	1	1	2	2	2	7	1	7	3	3	4
C_3	1	1	1	2	2	3	2	7	1	3	4	5	7
C_4	$\frac{1}{3}$	1	$\frac{1}{2}$	1	3	2	3	5	2	2	2	6	6
C_5	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{3}$	1	3	5	4	3	6	3	4	5
C_6	$\frac{1}{5}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{2}$	$\frac{1}{3}$	1	2	3	4	3	3	2	5
C_7	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{5}$	$\frac{1}{2}$	1	2	3	2	4	4	4
C_8	$\frac{1}{5}$	$\frac{1}{7}$	$\frac{1}{7}$	$\frac{1}{5}$	$\frac{1}{4}$	$\frac{1}{3}$	$\frac{1}{2}$	1	4	3	3	5	3
C_9	1	1	1	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{3}$	$\frac{1}{4}$	1	2	2	3	4
C_{10}	$\frac{1}{5}$	$\frac{1}{7}$	$\frac{1}{3}$	$\frac{1}{2}$	$\frac{1}{6}$	$\frac{1}{3}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{2}$	1	2	2	4
C_{11}	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{3}$	$\frac{1}{2}$	$\frac{1}{2}$	1	3	3
C_{12}	$\frac{1}{5}$	$\frac{1}{3}$	$\frac{1}{5}$	$\frac{1}{6}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{5}$	$\frac{1}{3}$	$\frac{1}{2}$	$\frac{1}{3}$	1	2
C_{13}	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{7}$	$\frac{1}{6}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{4}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{3}$	$\frac{1}{2}$	1

TABLE 9. Random index values.

Number of criteria	Random Index (R.I)
1	0
2	0
3	0.52
4	0.89
5	1.11
6	1.25
7	1.35
8	1.40
9	1.45
10	1.49
11	1.52
12	1.54
13	**1.56**

E. TOPSIS METHOD FOR EVALUATION OF SECURITY ATTRIBUTES

In this section, we perform some empirical work to validate the proposed framework by using TOPSIS method. In first section the TOPSIS method along with step-wise procedure has been discussed and in next section how this method in context of our research has been used will be discussed.

F. TOPSIS METHOD

The Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) was presented by Krohling and Pacheco [75]. This method works based on using ideal solution, if alternative is closer towards the positive ideal solution then it will considered as best solution. TOPSIS method follows simple computation procedure, it is well established and reliable [75]. In TOPSIS method the chosen alternative should have the shortest distance from the positive ideal solution and the farthest from the negative-ideal solution. In this research work, TOPSIS method is applied for assessment and ranking of IoHT devices. The following steps are used in TOPSIS method for ranking of alternatives [75], [76].

Step-1 Determine weight of decision making and constructing decision matrix

In this step, a decision matrix such as D is constructed by using multiple criteria and alternatives. For example for'' n'' number of alternatives and criteria, the decision matrix can be written as.

$$D = \begin{matrix} \\ A_1 \\ \vdots \\ A_n \end{matrix} \begin{bmatrix} C_1 & \ldots\ldots\ldots\ldots & C_n \\ X_{11} & \ldots\ldots\ldots & X_{1n} \\ & & \\ \vdots & \ddots & \vdots \\ X_{m1} & \ldots\ldots\ldots & X_{mn} \end{bmatrix} \tag{5}$$

where A_1, A_2, $A_{3.....}A_n$, are variable alternatives and C_1, C_2, $C_{3.....}C_n$ are the criteria.

Step-2 Construction of normalized decision matrix

The data of the decision matrix D comes from various sources, therefore, it has to be normalized to transform it into a dimensionless matrix. Dimension matrix allows the comparison of different criteria. A normalized decision matrix is built by using the following formula.

$$R_{ij} = \frac{X_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}} \tag{6}$$

For i=1.....m and j=1.....n

Step-3. Determining weighted normalized decision matrix

It is not necessary that all attributes must be of same importance. Therefore, a weighted normalized decision matrix is obtained by multiplying the each element of normalized decision matrix with a random weight number as given in formula below.

$$V = V_{ij} = W_j \times R_{ij}$$

$$V = \begin{bmatrix} V_{11} & V_{12} & V_{1j} & V_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ V_{i1} & V_{i2} & V_{ij} & V_{in} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ V_{m1} & V_{m2} & V_{mi} & V_{mn} \end{bmatrix} = \begin{bmatrix} w_1r_{11} & w_1r_{11} & w_1r_{11} & w_1r_{11} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ w_1r_{11} & w_1r_{11} & w_1r_{11} & w_1r_{11} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ w_1r_{11} & w_1r_{11} & w_1r_{11} & w_1r_{11} \end{bmatrix} \tag{7}$$

Step-4. Determining ideal positive and negative solutions

The positive ideal (A^+) and the negative ideal (A^-) solutions are defined according to the weighted decision matrix.

$$\begin{aligned} A^+ &= \left\{V_1^+, V_2^+, V_3^+, V_n\right\}, \text{ Where } V_j^+ \\ &= \left\{((\text{maxi}\left(V_{ij}\right) \text{if } j \in J); (\text{mini} V_{ij} \text{if } j \in J')\right\} \end{aligned} \tag{8}$$

$$\begin{aligned} A^- &= \left\{V_1^-, V_2^-, V_3^-, V_n^-\right\}, \text{ Where } V_j^- \\ &= \left\{(\text{mini}\left(V_{ij}\right) \text{if } j \in J); (\text{maxi} V_{ij} \text{if } j \in J')\right\} \end{aligned} \tag{9}$$

where, J denotes the beneficial attributes and J' is shows non-beneficial attributes.

Step-5. Calculation of separation measure

In this step ideal and no ideal separation are calculated by the following formulae.

$$S^+ = \sqrt{\sum_{J=1}^{n} (V_{ij} - V^+)^2} \quad \text{For i} = 1 \ldots .m \tag{10}$$

$$S^- = \sqrt{\sum_{J=1}^{n} (V_{ij} - V^-)^2} \quad \text{Fori} = 1 \ldots .m \tag{11}$$

Step-6. Measure the relative closeness of each location to the ideal solution

For each competitive alternative the relative closeness of the potential location with respect to the ideal solution is

TABLE 10. Normalized decision matrix table.

Alternatives	C_1	C_2	C_3	C_4	C_5	C_6	C7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}
D_1	0.44	0.61	0.53	0.55	0.40	0.58	0.49	0.58	0.50	0.41	0.45	0.44	0.46
D_2	0.50	0.48	0.47	0.48	0.46	0.41	0.49	0.49	0.50	0.52	0.45	0.55	0.54
D_3	0.56	0.41	0.53	0.55	0.53	0.50	0.37	0.58	0.44	0.41	0.51	0.55	0.46
D_4	0.50	0.48	0.47	0.41	0.59	0.50	0.62	0.29	0.56	0.62	0.58	0.44	0.54
C.W	**0.15**	**0.12**	**0.14**	**0.12**	**0.11**	**0.07**	**0.07**	**0.06**	**0.07**	**0.04**	**0.04**	**0.02**	**0.02**

TABLE 11. Weighted normalized table.

Alternatives	C_1	C_2	C_3	C_4	C_5	C_6	C7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}
D_1	0.063	0.071	0.072	0.063	0.045	0.040	0.033	0.033	0.033	0.015	0.016	0.010	0.009
D_2	0.072	0.055	0.064	0.055	0.053	0.029	0.033	0.028	0.033	0.019	0.016	0.013	0.011
D_3	0.081	0.047	0.072	0.063	0.060	0.034	0.025	0.033	0.029	0.015	0.018	0.013	0.009
D_4	0.072	0.055	0.064	0.047	0.068	0.034	0.041	0.017	0.038	0.022	0.020	0.010	0.011

computed.

$$C_i = \frac{S_{i^-}}{(S_i^+ + S_i^-)} 0 \le C_i \le 1 \tag{12}$$

Step-7. Ranking of alternatives or preference order

The ranking is done by using Ci value, the higher value of Ci means the higher the ranking order and alternative can be described as better in terms of performance. Ranking of the preference in descending order thus allows relatively better performances to be compared.

G. TOPSIS NUMERICAL WORK

In this section, we will assess four IoHT devices or equipments for security for 13 identified security requirements using TOPSIS method. The TOPSIS method is used for ranking alternatives (devices). Data relevant about security criteria is collected from the expert panel based upon Saaty's scale. A questionnaire is presented, which is answered by the experts in the field of IoT security. Decision matrix is constructed for IoHT devices and security requirements from expert panel. All the criteria are qualitative, so the quantitative data has been obtained for all IoT devices from expert panel by using scale ranges from 1 to 10. Based on this scaling the values out of 10 are given for alternatives against the security criteria as depicted in matrix (D) given below as.

Normalized decision matrix is obtained by using equation (6) and results are listed in Table 10 along with criteria weights (C.W), which are calculated by using AHP method in previous work. The data in decision matrix comes from different expert's opinions so it is important to normalize the data of decision matrix to convert it into dimensionless form.

Weighted normalized matrix is created by using equation (7) and results are given in Table 11. It is not necessary for each criteria to be of equal importance. For this purpose, weighted normalized decision matrix is obtained by multiplying each element of normalized decision matrix with a random weight number.

Ideal positive solution ($A^{+)}$ and ideal negative solution (A^-) are calculated by using equation (8) and equation (9) respectively and values are given in Table 12. The positive-ideal solution is composed of all best values attainable of criteria, and the negative-ideal solution consists of all the worst values attainable of criteria.

Positive ideal solutions and negative ideal solutions are used in finding ideal separation measures and non-ideal separation measures. These are calculated by using equations (10) and equation (11). Ideal separation measures (S^+) for D_1, D_2, D_3 and D_4 can be calculated as follow. Ideal separation measures are given in Table 13.

For each competitive alternatives i.e. D_1, D_2, D_3 and D_4, the relative closeness (Ci) of the potential location with respect to the ideal solution is computed by using equation (12). For each alternative such as D_1, D_2, D_3 and D_4, relative closeness of potential location with respect to ideal solution such as $C_i(D_1), C_i(D_2), C_i(D_3), C_i(D_4)$ are calculated as given below.

$$C_i(D_1) = \frac{0.037}{0.032 + 0.037} = \frac{0.037}{0.069} = 0.538$$

$$D = \begin{bmatrix} & C_1 & C_2 & C_3 & C_4 & C_5 & C_6 & C_7 & C_8 & C_9 & C_{10} & C_{11} & C_{12} & C_{13} \\ D_1 & 7 & 9 & 9 & 8 & 6 & 7 & 4 & 6 & 8 & 4 & 7 & 4 & 6 \\ D_2 & 8 & 7 & 8 & 7 & 7 & 5 & 4 & 5 & 8 & 5 & 7 & 5 & 7 \\ D_3 & 9 & 6 & 9 & 8 & 8 & 6 & 3 & 6 & 7 & 4 & 8 & 5 & 6 \\ D_4 & 8 & 7 & 8 & 6 & 9 & 6 & 5 & 3 & 9 & 6 & 9 & 4 & 7 \end{bmatrix}$$

TABLE 12. Positive ideal and negative ideal solutions.

	C_1	C_2	C_3	C_4	C_5	C_6	C7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}
A^+	0.081	0.071	0.072	0.063	0.068	0.040	0.041	0.033	0.038	0.022	0.020	0.013	0.011
A^-	0.063	0.047	0.064	0.047	0.045	0.029	0.025	0.017	0.029	0.015	0.016	0.010	0.009

TABLE 13. Ideal separation measures.

Ideal separation measures	D_1	D_2	D_3	D_4
S^+	0.032	0.031	0.032	0.031
S^-	0.037	0.022	0.022	0.033

TABLE 14. Ranking preferences.

Alternatives	D1	D2	D3	D4
Final score	**0.538**	0.417	0.516	0.518
Ranking	**1**	4	3	2

$$C_i(D_2) = \frac{0.022}{0.031 + 0.022} = \frac{0.022}{0.053} = 0.417$$
$$C_i(D_3) = \frac{0.034}{0.032 + 0.034} = \frac{0.034}{0.067} = 0.516$$
$$C_i(D_4) = \frac{0.033}{0.031 + 0.033} = \frac{0.033}{0.064} = 0.518$$

Based upon scoring of C_i, ranking is performed and higher value of C_i indicates best alternative among the four alternatives such as D_1, D_2, D_3 and D_4. After the calculation of relative closeness (C_i) then ranking is performed based upon the value of C_i. D_1 alternative has higher value among the other alternatives so it ranked as 1st based on higher value of C_i. The results of all alternatives based on higher score are given as $D_1 > D_4 > D_3 > D_2$ and their ranking preferences have been displayed in Table 14.

In Table 14, according to ranking D_1 alternative is higher in rank than other alternatives based upon the security requirements or criteria so it can be described as most reliable and secure IoT equipment in healthcare environment.

VI. CONCLUSION

The security of IoT is important due to its fast growing and multi-application nature. In this research work, a framework towards the security evaluation is applied for the security ranking of IoT devices in healthcare environment. This security evaluation framework is presented in light of using multi criteria decision making approaches. Requirements for security assessment are selected from both sources literature and ISO security standard. Then, MCDM methods such as AHP and TOPSIS are applied to validate the proposed framework. Weights are assigned by using AHP method and then TOPSIS method is used evaluate the security requirements for the ranking of alternatives. Precise and accurate results are obtained after the empirical work and these results can be used as metric of selecting the most reliable IoT solution in terms of security. This framework can be used for providing future guideline for selection of best security solution for IoHT based system and it can be used for making more suitable frameworks in future.

Our future work is to extend this framework by including more security requirements and alternatives and to use other multi criteria decision making approaches for assessment and decision making.

CONFLICT OF INTEREST

The authors declare no conflict of interest regarding this article.

REFERENCES

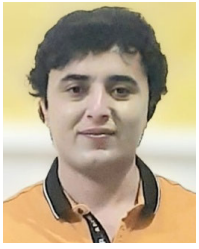
[1] S. Makkar, A. K. Singh, and S. Mohapatra, "Challenges and opportunities of Internet of Things for health care," in *A Handbook of Internet of Things in Biomedical and Cyber Physical System*. Berlin, Germany: Springer, 2019, pp. 301–314.
[2] Alliance of Advanced BioMedical Engineering, Frost & Sullivan. *Internet of Medical Things Revolutionizing Healthcare*. Accessed: Jul. 19, 2020. [Online]. Available: https://aabme.asme.org/posts/internet-of-medical-things-revolutionizing-healthcare
[3] *Internet of Medical Things (IoMT): New Era in Healthcare Industry*, Fuzon, Los Angeles, CA, USA, 2019.
[4] S. Elder. (2017). *87% of Healthcare Organizations Will Adopt Internet of Things Technology by 2019*. [Online]. Available: https://www.hipaajournal.com/87pc-healthcare-organizations-adopt-internet-of-things-technology-2019-8712/
[5] A. Arampatzis. (2019). *Protecting Modern IoMT Against Cybersecurity Challenges*. [Online]. Available: https://www.tripwire.com/state-of-security/healthcare/modern-iomt-cybersecurity-challenges/
[6] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and privacy in the Internet of medical things: Taxonomy and risk assessment," in *Proc. IEEE 42nd Conf. Local Comput. Netw. Workshops (LCN Workshops)*, Oct. 2017, pp. 112–120.
[7] J. D. Rockoff, "J&J warned insulin pump vulnerable to cyber hacking," *Wall Street J., Internet*, Jul. 2020. [Online]. Available: https://www.wsj.com/articles/j-j-warns-insulin-pump-vulnerable-to-cyber-hacking-1475610989?mg=prod/accounts-wsj
[8] A. Mondal, P. Rao, and S. K. Madria, "Mobile computing, IoT and big data for urban informatics: Challenges and opportunities," in *Handbook of Smart Cities*. Cham, Switzerland: Springer, 2018, pp. 81–113.
[9] S. Alam, M. M. R. Chowdhury, and J. Noll, "Interoperability of security-enabled Internet of Things," *Wireless Pers. Commun.*, vol. 61, no. 3, pp. 567–586, Dec. 2011.
[10] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.
[11] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of Things (IoT) security: Current status, challenges and prospective measures," in *Proc. 10th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2015, pp. 336–341.

[12] A. W. Atamli and A. Martin, "Threat-based security analysis for the Internet of Things," in *Proc. Int. Workshop Secure Internet Things*, Sep. 2014, pp. 35–43.
[13] K. C. Park and D.-H. Shin, "Security assessment framework for IoT service," *Telecommun. Syst.*, vol. 64, no. 1, pp. 193–209, Jan. 2017.
[14] R. Diesch, M. Pfaff, and H. Krcmar, "A comprehensive model of information security factors for decision-makers," *Comput. Secur.*, vol. 92, May 2020, Art. no. 101747.
[15] I. M. Abdelwahed, N. Ramadan, and H. A. Hefny, "Cybersecurity risks of blockchain technology," *Int. J. Comput. Appl. (0975–8887)*, vol. 177, no. 42, Mar. 2020.
[16] B. Song and S. Kang, "A method of assigning weights using a ranking and nonhierarchy comparison," *Adv. Decis. Sci.*, vol. 2016, pp. 1–9, Apr. 2016.
[17] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Bus. Horizons*, vol. 58, no. 4, pp. 431–440, Jul. 2015.
[18] M. Aly, F. Khomh, M. Haoues, A. Quintero, and S. Yacout, "Enforcing security in Internet of Things frameworks: A systematic literature review," *Internet Things*, vol. 6, Jun. 2019, Art. no. 100050.
[19] J. Ahamed and A. V. Rajan, "Internet of Things (IoT): Application systems and security vulnerabilities," in *Proc. 5th Int. Conf. Electron. Devices, Syst. Appl. (ICEDSA)*, Dec. 2016, pp. 1–5.
[20] C. Hosmer, "IoT vulnerabilities," in *Defending IoT Infrastructures With the Raspberry Pi: Monitoring and Detecting Nefarious Behavior in Real Time*. Berkeley, CA, USA: Apress, 2018, pp. 1–15.
[21] A. Tekeoglu and A. Ş. Tosun, "An experimental framework for investigating security and privacy of IoT devices," in *Proc. Int. Conf. Intell., Secure, Dependable Syst. Distrib. Cloud Environ.*, 2017, pp. 63–83.
[22] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018.
[23] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "SoK: Security evaluation of home-based IoT deployments," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019, pp. 1362–1380.
[24] M. Chernyshev and P. Hannay, "Security assessment of IoT devices: The case of two smart TVs," in *Proc. 13th Austral. Digit. Forensics Conf.* Perth, WA, Australia: Edith Cowan Univ. Joondalup Campus, Nov./Dec. 2015, pp. 85–94. [Online]. Available: https://ro.ecu.edu.au/adf/153 https://ro.ecu.edu.au/adf/153, doi: 10.4225/75/57b3fa87fb88d.
[25] B. Ali and A. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *Sensors*, vol. 18, no. 3, p. 817, Mar. 2018.
[26] O. Mazhelis and P. Tyrvainen, "A framework for evaluating Internet-of-Things platforms: Application provider viewpoint," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 147–152.
[27] W. Xi and L. Ling, "Research on IoT privacy security risks," in *Proc. Int. Conf. Ind. Informat.-Comput. Technol., Intell. Technol., Ind. Inf. Integr. (ICIICII)*, Dec. 2016, pp. 259–262.
[28] S. S. Rani, J. A. Alzubi, S. K. Lakshmanaprabu, D. Gupta, and R. Manikandan, "Optimal users based secure data transmissionon the internet of healthcare things (IoHT) with lightweight blockciphers," *Multimedia Tools Appl.*, vol. 18, no. 3, pp. 1–20, 2019.
[29] W. Leister, M. Hamdi, H. Abie, S. Poslad, and A. Torjusen, "Anevaluation framework for adaptive security for the IoT in ehealth," *Int. J. Adv. Secur.*, vol. 7, nos. 3–4, pp. 93–109, 2014.
[30] D. Nkomo and R. Brown, "Hybrid cybersecurity framework for the Internet of medical things (IOMT)," in *Proc. IEEE 12th Int. Conf. Global Secur., Saf. Sustainability (ICGS)*, Jan. 2019, p. 212.
[31] M. A. Jan, M. Usman, X. He, and A. U. Rehman, "SAMS: A seamless and authorized multimedia streaming framework for WMSN-based IoMT," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1576–1583, Apr. 2019.
[32] M. Usman, M. A. Jan, X. He, and J. Chen, "P2DCA: A privacy-preserving-based data collection and analysis framework for IoMT applications," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 6, pp. 1222–1230, Jun. 2019.
[33] D. Rizk, R. Rizk, and S. Hsu, "Applied layered-security model to IoMT," in *Proc. IEEE Int. Conf. Intell. Secur. Informat. (ISI)*, Jul. 2019, p. 227.
[34] J. Cecil, A. Gupta, M. Pirela-Cruz, and P. Ramanathan, "An IoMT based cyber training framework for orthopedic surgery using next generation Internet technologies," *Informat. Med. Unlocked*, vol. 12, pp. 128–137, 2018.
[35] M. A. Bilal and M. A. Hassan, "A distributed secure framework for sharing patient's data among IoMT devices," *Pakistan J. Eng. Appl. Sci.*, vol. 24, no. 1, pp. 1–12, Oct. 2019.
[36] S. Liaqat, A. Akhunzada, F. S. Shaikh, A. Giannetsos, and M. A. Jan, "SDN orchestration to combat evolving cyber threats in Internet of medical things (IoMT)," *Comput. Commun.*, vol. 160, pp. 697–705, Jul. 2020.
[37] H. Jahankhani and J. Ibarra, "Digital forensic investigation for the Internet of medical things (IoMT)," *Forensic Leg. Investig. Sci.*, vol. 5, no. 2, p. 029, Aug. 2019, doi: 10.24966/FLIS-733X/100029.
[38] X. Li, H.-N. Dai, Q. Wang, M. Imran, D. Li, and M. A. Imran, "Securing Internet of medical things with friendly-jamming schemes," *Comput. Commun.*, vol. 160, pp. 431–442, Jul. 2020.
[39] T. D. C. Frazão, D. G. G. Camilo, E. L. S. Cabral, and R. P. Souza, "Multicriteria decision analysis (MCDA) in health care: A systematic review of the main characteristics and methodological steps," *BMC Med. Informat. Decis. Making*, vol. 18, no. 1, p. 90, Dec. 2018.
[40] J. I. Drake, J. C. T. de Hart, C. Monleón, W. Toro, and J. Valentim, "Utilization of multiple-criteria decision analysis (MCDA) to support healthcare decision-making FIFARMA, 2016," *J. Market Access Health Policy*, vol. 5, no. 1, Jan. 2017, Art. no. 1360545.
[41] Y. Liu, Y. Yang, Y. Liu, and G.-H. Tzeng, "Improving sustainable mobile health care promotion: A novel hybrid MCDM method," *Sustainability*, vol. 11, no. 3, p. 752, Jan. 2019.
[42] F. Alsubaei, A. Abuhussein, V. Shandilya, and S. Shiva, "IoMT-SAF: Internet of medical things security assessment framework," *Internet Things*, vol. 8, Dec. 2019, Art. no. 100123.
[43] W.-H. Liao and W.-L. Qiu, "Applying analytic hierarchy process to assess healthcare-oriented cloud computing service systems," *SpringerPlus*, vol. 5, no. 1, p. 1030, Dec. 2016.
[44] F. Alsubaei, A. Abuhussein, and S. Shiva, "A framework for ranking IoMT solutions based on measuring security and privacy," in *Proc. Future Technol. Conf.*, 2018, pp. 205–224.
[45] M. Rajasekaran, A. Yassine, M. S. Hossain, M. F. Alhamid, and M. Guizani, "Autonomous monitoring in healthcare environment: Reward-based energy charging mechanism for IoMT wireless sensing nodes," *Future Gener. Comput. Syst.*, vol. 98, pp. 565–576, Sep. 2019.
[46] R. Kumar, A. K. Pandey, A. Baz, H. Alhakami, W. Alhakami, A. Agrawal, and R. A. Khan, "Fuzzy-based symmetrical multi-criteria decision-making procedure for evaluating the impact of harmful factors of healthcare information security," *Symmetry*, vol. 12, no. 4, p. 664, Apr. 2020.
[47] N. Dimitrioglou, D. Kardaras, and S. Barbounaki, "Multicriteria evaluation of the Internet of Things potential in health care: The case of dementia care," in *Proc. IEEE 19th Conf. Bus. Informat. (CBI)*, Jul. 2017, pp. 454–462.
[48] F. A. Al-Zahrani, "Evaluating the usable-security of healthcare software through unified technique of fuzzy logic, ANP and TOPSIS," *IEEE Access*, vol. 8, pp. 109905–109916, 2020.
[49] M. Rajak and K. Shaw, "Evaluation and selection of mobile health (mHealth) applications using AHP and fuzzy TOPSIS," *Technol. Soc.*, vol. 59, Nov. 2019, Art. no. 101186.
[50] G. Büyüközkan and G. Çifçi, "A combined fuzzy AHP and fuzzy TOPSIS based strategic analysis of electronic service quality in healthcare industry," *Expert Syst. Appl.*, vol. 39, no. 3, pp. 2341–2354, Feb. 2012.
[51] Ž. Rađenović and I. Veselinović, "Integrated AHP-TOPSIS method for the assessment of health management information systems efficiency," *Econ. Themes*, vol. 55, no. 1, pp. 121–142, Mar. 2017.
[52] A. Hinduja and M. Pandey, "An ANP-GRA-eased evaluation model for security features of IoT systems," in *Intelligent Communication, Control and Devices*. Singapore: Springer, 2020, pp. 243–253.
[53] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, Feb. 2018.
[54] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the Internet of Things," in *Proc. IEEE World Congr. Services*, Jun. 2015, pp. 21–28.
[55] H.-J. Kim, H.-S. Chang, J.-J. Suh, and T.-S. Shon, "A study on device security in IoT convergence," in *Proc. Int. Conf. Ind. Eng., Manage. Sci. Appl. (ICIMSA)*, May 2016, pp. 1–4.
[56] L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, and J. J. C. de Santanna, "Internet of Things in healthcare: Interoperatibility and security issues," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 6121–6125.
[57] I. Alqassem and D. Svetinovic, "A taxonomy of security and privacy requirements for the Internet of Things (IoT)," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage.*, Dec. 2014, pp. 1244–1248.
[58] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2014, pp. 417–423.
[59] M. Abdur, S. Habib, M. Ali, and S. Ullah, "Security issues in the Internet of Things (IoT): A comprehensive study," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 6, pp. 383–388, 2017.

[60] C. Lee, L. Zappaterra, K. Choi, and H.-A. Choi, "Securing smart home: Technologies, security challenges, and security requirements," in *Proc. IEEE Conf. Commun. Netw. Secur.*, Oct. 2014, pp. 67–72.
[61] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed security model and threat taxonomy for the Internet of Things (IoT)," in *Proc. Int. Conf. Netw. Secur. Appl.*, 2010, pp. 420–429.
[62] B.-C. Chifor, I. Bica, V.-V. Patriciu, and F. Pop, "A security authorization scheme for smart home Internet of Things devices," *Future Gener. Comput. Syst.*, vol. 86, pp. 740–749, Sep. 2018.
[63] S. Hameed, F. I. Khan, and B. Hameed, "Understanding security requirements and challenges in Internet of Things (IoT): A review," *J. Comput. Netw. Commun.*, vol. 2019, pp. 1–14, Jan. 2019.
[64] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, and Y. Jin, "Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice," *J. Hardw. Syst. Secur.*, vol. 2, no. 2, pp. 97–110, Jun. 2018.
[65] M. G. Samaila, M. Neto, D. A. B. Fernandes, M. M. Freire, and P. R. M. Inácio, "Challenges of securing Internet of Things devices: A survey," *Secur. Privacy*, vol. 1, no. 2, p. e20, Mar. 2018.
[66] S. Ziegler, C. Crettaz, E. Kim, A. Skarmeta, J. B. Bernabe, R. Trapero, and S. Bianchi, "Privacy and security threats on the Internet of Things," in *Internet of Things Security and Data Protection*. Cham, Switzerland: Springer, 2019, pp. 9–43.
[67] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019.
[68] C. Okoli and S. D. Pawlowski, "The delphi method as a research tool: An example, design considerations and applications," *Inf. Manage.*, vol. 42, no. 1, pp. 15–29, Dec. 2004.
[69] D. Pamučar, Ž. Stević, and S. Sremac, "A new model for determining weight coefficients of criteria in MCDM models: Full consistency method (FUCOM)," *Symmetry*, vol. 10, no. 9, p. 393, Sep. 2018.
[70] M. S. D. Putra, S. Andryana, Fauziah, and A. Gunaryati, "Fuzzy analytical hierarchy process method to determine the quality of gemstones," *Adv. Fuzzy Syst.*, vol. 2018, pp. 1–6, Oct. 2018.
[71] F. G. M. Al-Azab and M. A. Ayu, "Web based multi criteria decision making using AHP method," in *Proc. 3rd Int. Conf. Inf. Commun. Technol. Moslem World (ICTM)*, Dec. 2010, pp. A6–A12.
[72] S. K. Sehra, D. Y. S. Brar, and D. N. Kaur, "Multi criteria decision making approach for selecting effort estimation model," 2013, *arXiv:1310.5220*. [Online]. Available: http://arxiv.org/abs/1310.5220
[73] S. S. S. Nazir and S. B. S. Abid, "Selecting software design based on birthmark," *Life Sci. J.*, vol. 11, no. 12, pp. 1–5, 2014.
[74] T. L. Saaty and L. T. Tran, "On the invalidity of fuzzifying numerical judgments in the analytic hierarchy process," *Math. Comput. Model.*, vol. 46, nos. 7–8, pp. 962–975, Oct. 2007.
[75] R. A. Krohling and A. G. C. Pacheco, "A-TOPSIS—An approach based on TOPSIS for ranking evolutionary algorithms," *Procedia Comput. Sci.*, vol. 55, pp. 308–317, Jan. 2015.
[76] P. Wang, B. Li, H. Shi, Y. Shen, and D. Wang, "Revisiting anonymous two-factor authentication schemes for IoT-enabled devices in cloud computing environments," *Secur. Commun. Netw.*, vol. 2019, pp. 1–13, May 2019.

LANJING WANG was born in Henan, China, in 1975. He received the B.M. degree in library science from Zhengzhou University, Henan, the M.S. degree in basic mathematics from Henan University, Henan, in 2008, and the Ph.D. degree in management from Nanjing University, Jiangsu, China, in 2012. From 2013 to 2015, he was a Lecturer with the School of Business, Henan University, where he has been an Associate Professor, since 2016. He is the author of one book, more than 20 articles. His research interests include logistics information management, innovation management, and digital economy.

YASIR ALI received the M.Sc. degree in computer science from the University of Peshawar. He is currently pursuing the M.S. degree in computer science with the Department of Computer Science, University of Swabi. He is also working as a Lecturer with the Government Postgraduate College, Swabi. His research interests include the Internet of Things and security evaluation.



SHAH NAZIR received the Ph.D. degree in computer science with a specialization in software engineering. He has worked at the University of Peshawar. He is currently serving as an Assistant Professor and the Head of the Department of Computer Science, University of Swabi. He has several research publications in well-reputed international journals and conference proceedings. His research interests include component-based software engineering, software birthmark, systematic literature review, and decision making. He is a reviewer of several journals and conferences.

MAHMOOD NIAZI is currently an Associate Professor of software engineering with the Information and Computer Science Department, King Fahd University of Petroleum and Minerals, Saudi Arabia. He has spent over a decade with leading technology firms and universities as a Process Analyst, a Senior Systems Analyst, the Project Manager, a Lecturer, and a Professor. He has participated in and managed several software development projects. He has published over 100 articles in peer-reviewed conferences and journals. His research interests include evidence-based software engineering, requirements engineering, sustainable, reliable, and secure software engineering processes, global system development and management, project management, and software process improvement. His work has received over 3000 citations and has received awards for best papers at several conferences.