Webology (ISSN: 1735-188X)
Volume 18, Number 2, 2021

A Novel Model For Implementing Internet Of Things (Iot) In Iranian Hospitals: A Cross Sectional Study Based On The Challenges Of Using Iot In Health Systems

Khadijeh Moulaei [1] , Shirin Ayani [2] , Kambiz Bahaadinbeigy [3*], Rafat Bayat [4] , Farhad Fatehi[5, 6] , Farahnaz Sadoughi[7]

[1]Ph.D candidate in medical informatics, Student Research Committee, Kerman University of Medical Sciences, Kerman, Iran.

[2]Smart Hospital and e-Health Research and Development Center, Raymand e-Health Company, Tehran, Iran.

[3]* MD, Ph.D , Associate Professor of Medical Informatics. Medical Informatics Research Center, Institute for Futures Studies in Health, Kerman University of Medical Sciences, Kerman, Iran.

[4]Ph.D in Sociology, Manager of Faran Mehre Danesh Virtual Higher Education Inst, Tehran, Iran.

[5]Centre for Online Health, The University of Queensland, Brisbane, Australia.

[6]School of Psychological Sciences, Monash University, Melbourne, Australia.

[7]Professor of Health Information Management, Health Management and Economics Research Center, School of Health Management and Information Sciences, Iran University of Medical Sciences, Tehran, Iran.

Abstract

The internet of things (IOT) has led to ground-breaking changes in the healthcare industry as a promising technological solution. Yet, despite its many benefits, its application has always proven to be challenging. Therefore, the aim of this study was to identify the challenges of using internet of things in health systems with the aim of providing a model for implementing IoT in Iranian hospitals. This study was performed in three phases. In the first phase, the challenges of using the IoT were identified In the second phase, according to experts, this challenge was confirmed during the completion of a two-round Delphi. In the last phase, a novel model for implementing the IoT in Iranian hospitals was proposed. The model consisted of six groups, namely privacy and security, big data, hardware, network, software, and organizational-cultural and environmental challenges. Out of the 78 identified challenges, 46 were approved by experts as essential elements for providing IoT model in Iranian hospitals. The highest and lowest averages were related to the subgroups "Failure to provide regular IoT rules and programs by governments" and "Absence of single, integrated and efficient platforms with high data transfer capacity and fast data processing", respectively. The final model for implementing IoT in Iranian hospitals was designed and presented using Edraw Max10.0.4+Portable software. Challenges identified and this model can provide a sufficient basis, information and knowledge for policymakers, government authorities and managers of organizations to use the IoT in hospitals of Iran and other countries. Also, the proposed model can also improve special capabilities in system design; reduce failure in the initial design of IoT projects, and save time and money.

Keywords: Internet of Things (IoT); hospitals; model; challenges; health care

Introduction

Over the past two decades, although health care systems around the world have undergone profound changes (Kisa, 2008), but most of these systems in many countries are of poor quality, slow, and inevitably prone to error. These issues are obviously quite solvable, as healthcare organizations rely on countless activities and devices that can be automatically enhanced through state-of-the-art technology (Hussein, 2019). As one of the world's most top technologies, the Internet of Things (IoT) is currently billed the most promising solution for the healthcare industry (Joyia, Liaqat, Farooq, & Rehman, 2017), which can transform the healthcare industry by increasing efficiency, improving the quality of various services and optimizing healthcare costs (Rghioui & Oumnad, 2018). IoT plays a critical role in the healthcare industry, which is achieved by increasing accuracy and reliability, and the application of electronic devices (Joyia et al., 2017). This technology saves people's time and money through its numerous capabilities, improves decision-making processes, and improves people's health by automating and strengthening various activities (Ifrim, Pintilie, Apostol, Dobre, & Pop, 2017). Furthermore, smart and cost-effective IoT powers and facilitates health care systems, thus improving the quality of health care and potentially saving patients' lives and reducing overall healthcare costs (Gia, Rahmani, Westerlund, Liljeberg, & Tenhunen, 2015).

Despite the many benefits of IoT technology, the persistence of some challenges has made its implementation a serious concern (Upadhyay, 2018). Experts in the field believe that the challenges of the internet of things are too many and far-fetched (Sundmaeker, Guillemin, Friess, & Woelfflé, 2010). This technology has to deal with a plethora of important challenges such as maintaining security and privacy (T. Devendran, 2018), confidentiality, safe and secure network communication, energy saving, information retention, identification and authentication of users, evaluation and monitoring of components, ensuring secure information exchange and trust between the various infrastructures of vertical information technology (Albishi, Soh, Ullah, & Algarni, 2017). Other challenges, such as big data, networking, energy and power consumption, interactivity, scalability, heterogeneity, security and privacy, and maintenance, can all hinder the successful deployment of IoT applications (Atlam, Walters, & Wills, 2018).

Zeadally et al. (Zeadally, Siddiqui, Baig, & Ibrahim, 2019) argued that before digital health care could develop stable, flexible, and interactive systems, the corresponding challenges should first be addressed, an effort which necessitates identifying technology-related challenges. It is also noteworthy that although the use of IoT is rapidly spreading around the world as an emerging phenomenon (Rghioui & Oumnad, 2018), like other technologies, this technology is prone to the underlying challenges. Therefore, the purpose of this study is to identify the various challenges of using the internet of things so as to provide a model for implementing the IoT in Iranian hospitals. Since no such study has been undertaken in Iran, conducting this research and applying effective scientific and technical policies in various organizations in the field of health can either solve or at least minimize existing challenges. The contributions can also maximize the potential of employing IoT-based technologies to improve and enhance people's health, reducing large-scale costs in the healthcare industry, integrating medical equipment and systems, and tracking patients, staff, and hospital equipment.

Methods

The present study was performed in three phases: (1) Identifying and introducing the challenges of employing the internet of things in the health systems; (2) Final confirmation of these challenges by the experts; and (3) Designing and proposed a model for implementing the IoT in Iranian hospitals.

Phase 1: Identifying and introducing the challenges of using the Internet of things

In this phase to extract the IoT challenges, a comprehensive search was conducted from 10 to 30 February 2020 at the IEEE, PubMed and Web of Science. The keywords and the search strategy are listed in table 1.

Table 1. Keywords and search strategy

No.	Keywords
1	(Internet of Things (IOT) OR Internet of Healthcare Things OR Medical Internet of Things (M-IOT) OR Wearable electronic devices OR Body Sensor Networks(BSN) OR Body Area Network (BAN) OR wearable sensors OR wearable devices)
2	(Challenges OR Issues OR Problems)
3	Healthcare OR Health Information Systems OR e-health
Search strategy	[(1) AND (2) AND (3)]

Inclusion and exclusion criteria

Articles were included in this study based on the following criteria: being published in English, availability of full-text articles, and pointing out the challenges of using the IoT in healthcare systems.

The exclusion criteria also included articles regarding other aspects of the IoT, and the lack of clear information about the challenges of using the IoT in healthcare. Moreover, books and books chapters, letters to the editors, and abstracts of the conferences were excluded.

Classification and selecting resources

At this stage, the data were collected by a data extraction form. The validity of this form was confirmed by two medical informatics and one health information management experts. The full texts of the articles were studied. Finally, the challenges of using the internet of things in health systems were extracted.

Then, challenges and their scope were approved and classified according to the opinion of at least five experts in computer engineering (2 people), medical informatics (2 people) and health information management (1 people). After the formation of the theoretical framework and reviewing and studying the existing questionnaires in Iran and other countries, basic parameters and items were compiled and a questionnaire was created.

Phase 2: Final approval of the challenges of employing the Internet of Things in the health systems according to experts

In this phase, a questionnaire was used to obtain the opinion of experts. The designed questionnaire consisted of two sections. The first section was related to participant's demographic information. The second section included 78 items related to the IoT challenges identified in the six groups: Privacy and security challenges, big data, hardware, network, software, and organizational-cultural and environmental. It should be noted that an open question titled "Other Challenges" was included at the end of the questionnaire in order to receive other opinions and suggestions of the experts.

The face and content validity of the questionnaire was confirmed by two medical informatics experts, two experts in the field of health information management and a software engineer. Also, the reliability of the questionnaire was calculated with Cronbach's alpha formula to be 0.947. In order to analyze the data for each part of the questionnaire, each item was scored based on a 5-level Likert scale: "very high", "high", "medium", "low" and "very low". Therefore, the scoring scale for each of the challenges was measured to be between one and five (Faber-Wildeboer, van Os-Medendorp, Kooy, & Sol-De Rijk, 2013; Moulaei, Malek, & Sheikhtaheri, 2019).

Owing to the fact that in most Delphi studies, the number of experts sits in the range of 15 to 20, the sampling was done randomly(Hsu & Sandford, 2007). We sent an invitation to 40 medical informatics, health information management and computer engineering (software or hardware) experts working in the IT department of Iranian hospitals. Twenty-five experts accepted our invitation. Finally, according to the inclusion criteria, 20 experts were selected to participate in the study.

Following inclusion criteria were considered for experts of the study:

- Having at least a bachelor's degree
- Working in the IT department of the hospitals for at least five years
- Being familiar with the concept of the Internet of Things

- Having specializations in software engineering, hardware, medical informatics or health information management

In the first stage Delphi, the researcher first provided the necessary explanations (about the aims of the study and how to complete the questionnaire) for each participant through telephone communication or social media. Then, the questionnaires were distributed electronically among the experts.

In the first stage Delphi, the questionnaires were distributed and collected among experts from March 24 2020 to April 19 2020. The questionnaires in the second stage Delphi were distributed and collected electronically among the same Delphi specialists of the first stage one month after Delphi of the first stage, i.e. May 19 2020. After collecting the questionnaires, the data were imported to SPSS 23, and then the frequency and mean of each item were calculated and analyzed. After gaining the frequency and mean of the first round of Delphi, the opinions of the experts were examined and analyzed. In order to decide on each challenge in the first stage, an agreement level was considered. As such, challenges with an mean of less than 50 percent in the first round were excluded at the study, challenges with a mean of 50 to 75 percent entered the second stage Delphi, and challenges with a mean of more than 75 percent were considered as the final challenges of the proposed model without further need for being pressured in the second stage Delphi. (Moulaei, Bahaadinbeigy, & Fatehi, 2021, Chraghbaigi, Fathi, & Shojaee Baghini, 2014).

Phase 3: Designing and presenting a model for implementing the Internet of Things in Iranian hospitals

Initially, several samples of IoT reference models were studied with the purpose of gaining a primary insight and consequently designing and proposing a model for IoT implementation in Iranian hospitals (Bakhshi, Balador, & Mustafa, 2018; Modarresi, Gangadhar, & Sterbenz, 2017; Weyrich & Ebert, 2015). Then, according to the identified challenges and sample studies, the reference model from Cisco Inc was used as the basis for the model, based on which a prototype model was devised ("Tracking the Internet of Things for the Australian IT community"). In the next step, during several tele-conference meeting between the members of the research team, the prototype was explained and analyzed. Finally, the final model of IoT implementation in Iranian hospitals was designed and presented using Edraw Max 10.0.4 + Portable software.

Results

- **Final identified and validated challenges**

One thousand nine hundred articles were extracted from the three databases of IEEE and PubMed, Web of Science. Then, according to the inclusion and exclusion criteria's, 70 articles were eventually considered. Finally, 78 challenges were identified of articles. The identified challenges are classified and listed in Table 4.

The demographic information of participants is presented in Table 1. The frequency of male participants (65%) was higher than women. The highest age group was assigned to people aged 25 to 35. The frequency of medical informatics experts (55%) was higher than the other two groups.

Table 2. Participants' demographics

Variables		**Frequency**	Percentage
Sex	Male	13	65
	Female	7	35
Age	25-35	8	40
	36-45	7	35
	46-55	5	25
Education level	Bachelor	3	15
	MSc	8	40
	PhD	9	45
Experts	Engineering (Hardware / Software)	7	35
	Medical informatics	11	55
	Health information management (HIM)	2	10
Years of service	1-10	7	35
	11-21	11	55
	>21	2	10

Seventy-eight identified challenges were divided into six groups according to the opinions and experiences of the research experts (Table 3). Of the 78 challenges identified, 46 were eventually confirmed by experts as the main challenges for designing and deploying a model for employing the internet of things in Iranian hospitals. Thirty-two challenges were excluded during Delphi's first and second rounds. Forty eight challenges acquired a mean of 50 to 75 percent in the first stage Delphi and thus entered the second round. Of the 48 challenges in the second round of Delphi, 32 items with a mean in the range of 50-75% were excluded from the study.

Table 3. Main and subgroups (Identified Challenges) in Delphi, first and second rounds

Main groups	**The Number of subgroups**	**First Round of Delphi**			**Second Round of Delphi**			**The Number of final subgroups**
		< 50%	**50-75%**	**>75%**	**< 50%**	**50-75%**	**>75%**	
Privacy and security	14	0	12	2	0	1	11	13

Big data	10	0	6	4	0	3	3	7
Hardware	13	0	8	5	0	8	0	5
Network	19	0	15	4	0	13	2	6
Software	8	0	5	3	0	5	0	3
Organizational, cultural, environmental	14	0	2	12	0	2	0	12

According to Tables 3 and 4, the group of hardware challenges and the organizational-cultural and environmental challenges were the only groups of which 8 and 2 subgroups respectively were not approved in the first and second rounds of Delphi. Also, among the groups, the challenges associated with groups of privacy and security, and organizational-cultural and environmental issues were approved by experts with the most subgroups. The group with the highest number of excluded challenges and subgroups was the network group. The highest mean in the first round Delphi were associated with the subgroups of failure to provide regular IoT rules and programs by governments with an mean of 4.40, negligence of governments with an mean of 4.33 and reluctance of organizations, physicians and other employees in using novel technologies with an mean of 4.30 from the organizational-cultural and environmental group. In the second round Delphi, downloading or using inefficient and unauthorized programs with a mean of 4.33, difficult updates to security protocols with a mean of 4.13 and lack of mechanism to detect and prevent intrusion attacks (attacks such as Trojans, viruses and malware)" with a mean of 4.27 from the main privacy group were introduced as the most important challenges.

Among the accepted subgroups, the lowest mean in first round Delphi were related to the absence of single, integrated and efficient platforms with high data transfer capacity and fast processing with a mean of 3.76. In the second round Delphi, the persistence of malicious cyber attacks from the privacy and security group were introduced as the least important challenges with a mean of 3.80.

Table 4. Challenges of using IoT in health systems in Delphi, first and second stage

		1nd round Delphi		**2nd round Delphi**	
Main groups	**Subgroups (Identified Challenges)**	**Mean(±SD)**	**Subgroups rejected or entered in second round Delphi**	**Mean(±SD)**	**Final subgroups rejected or accepted**
Privacy and security	Lack of security design for protecting the network, systems and information from any intrusion	3.81(±0.92)	√		√
	Use of weak encryption algorithms and techniques	3.45(±1.07)	*	3.93(±0.96)	√

	Poor security of information, systems and equipment	3.80(±1.07)	√		√
	Preserving information confidentiality	3.42(±0.98)	*	4.00(±1.06)	√
	Illegal disclosure of information	3.48(±0.98	*	3.87(±0.91)	√
	Illegal access to systems and information	3.38(±1.07)	*	3.87(±0.91)	√
	Difficult updates to security protocols	3.30(±1.08)	*	4.13(±0.74)	√
	Lack of privacy	3.52(±1.16)	*	3.84(±0.94)	√
	Lack of authentication and identification of individuals	2.86(±0.91)	*	4.13(±0.74)	√
	Persistence of malicious cyber attacks	3.52(±0.87)	*	3.80(±1.08)	√
	Penetrating the organization and systems through malware	3.19(±0.98)	*	4.07(±0.88)	√
	Lack of mechanism to detect and prevent intrusion attacks (attacks such as Trojans, viruses and malware)	3.38(±1.20)	*	4.27(±0.77)	√
	Downloading or using inefficient and unauthorized programs	3.14(±0.91)	*	4.33(±0.61)	√
	Hacking systems and gaining access to data and systems	3.38(±0.92)	*	3.73(±0.96)	×
Big data	Difficult management and integration of data	4.24(±0.70)	√		√
	Big data processing	4.24(±0.62)	√		√
	Big data storage	3.81(±0.92)	√		√
	The existence of data heterogeneity owing to acquisition from different sources	4.15(±0.74)	√		√
	Weak and inefficient management of Big data	3.71(±1.07)	*	4.00(±0.75)	√
	High volume of data and data traffic	3.71(±1.07)	*	4.13(±0.64)	√
	Loss of data and loss during storage or transfer	3.14(±1.10)	*	3.87(±0.99)	√
	Backup of big data	3.19(±1.07)	*	3.07(±1.28)	×
	Lack of secure high-quality databases for storing metadata	3.70(±1.12)	*	3.53(±0.99)	×

	Lack of validation of data after acquisition from equipment	3.43(±0.97)	*	3.73(±1.03)	×
Hardware	Lack of powerful and high-quality equipment	3.86(±0.96)	√		√
	Lack of update and upgrade of the organizational equipment	3.86(±0.85)	√		√
	Lack of validation and approval of equipment installed in the organization	3.86(±0.79)	√		√
	Lack of ideal and suitable hardware equipment	3.90(±1.04)	√		√
	Incompatibility in the integration and development shifts of traditional and old systems to IoT-based systems and configurations	4.10(±0.99)	√		√
	Low battery life of equipment and power supply	3.10(±1.26)	*	3.67(±1.17)	×
	Weak computing power of systems in data processing and analysis	3.62(±0.92)	*	3.47(±1.24)	×
	Disruption of equipment due to noise	3.00(±1.00)	*	3.60(±1.18)	×
	Poor performance and low CPU frequency	3.45(±0.99)	*	2.87(±1.18)	×
	Disconnection of equipment from each other	3.52(±1.16)	*	3.20(±1.20)	×
	Memory and storage space constraints on equipment	3.67(±0.91)	*	3.40(±1.12)	×
	Fault tolerance (delays in service delivery and tolerance in the event of problems and errors, mainly hardware)	3.62(±0.86)	*	3.60(±0.98)	×
	Extensive heterogeneity between systems and equipment	3.71(±1.00)	*	3.60(±0.98)	×
Network	The high cost of purchasing hardware and systems	4.10(±0.91)	√		√
	Scalability	3.85(±0.87)	√		√
	Lack of proper communication infrastructure	4.10(±1.04)	√		√
	Incompatibility in merging and integrating network equipment with each other	3.81(±1.03)	√		√

	Hardware and network equipment failure	3.19(±0.75)	*	3.67(±1.13)	×
	Server failure or interruption	3.10(±1.13)	*	4.00(±1.13)	√
	Lack of dynamic network topology (a health device may connected to IoT health network at any location or any time)	3.29(±1.27)	*	3.87(±0.91)	√
	Difficult management and control of network equipment	3.25(±0.91)	*	3.60(±1.05)	×
	Disregarding wireless connections for connecting to a local or global network	3.19(±1.03)	*	3.53(±0.99)	×
	Failure to use appropriate routing protocols and algorithms for sending information	3.20(±1.19)	*	3.53(±1.06)	×
	Lack of powerful, ideal and convenient hardware	3.71(±1.05)	*	3.20(±1.14)	×
	Low computing power and power in data processing and analysis	3.38(±0.97)	*	3.53(±1.30)	×
	Poor internet connection	3.24(±1.26)	*	3.73(±1.28)	×
	Failure to select the appropriate network type for data sharing	3.19(±1.16)	*	3.53(±1.18)	×
	Difficult sharing and exchange of data and information on the network	3.00(±1.04)	*	2.93(±0.96)	×
	Ignoring cloud computing techniques for storage	3.57(±1.43)	*	3.20(±1.01)	×
	Disruption of transmission media due to noise	2.76(±0.83)	*	3.33(±1.11)	×
	Low bandwidth	3.71(±1.10)	*	3.73(±1.16)	×
	Difficulty in bandwidth sharing	3.71(±1.23)	*	3.13(±1.12)	×
Software	Poor interaction between systems	3.86(±1.10)	√		√
	Lack of integration of sustainable and useful tele-homecare services with hospital systems	4.14(±0.96)	√		√
	Absence of single, integrated and efficient platforms with high data transfer capacity and fast processing	3.76(±1.07)	√		√
	Complexity of software systems (non-friendly interface)	3.38(±1.02)	*	3.67(±1.04)	×

	Lack of regular updating of software programs and databases	3.71(±1.00)	*	3.40(±0.63)	×
	Lack of integration of installed operating systems and applications	3.19(±1.16)	*	3.47(±1.06)	×
	Lack of efficient and real-time operating systems	3.71(±1.18)	*	3.53(±1.30)	×
	Poor data compression	3.00(±0.94)	*	3.47(±0.83)	×
Organizational, cultural, environmental	Lack of clear rules on accessing to data usage equipment	3.86(±0.96)	√		√
	Lack of clear rules and standards for IoT equipment developers	4.00(±0.85)	√		√
	Weak influence of the organization in the market of wearable equipment and systems	3.95(±0.86)	√		√
	Adopting inappropriate and new policies in line with IoT healthcare business	3.78(±1.09)	√		√
	Reluctance of organizations, doctors and other employees in using novel technologies	4.30(±0.73)	√		√
	Lack of awareness, skills and poor knowledge of users regarding the implementation, application and use of IoT technologies	4.10(±0.99)	√		√
	Lack of specialized personnel in the organization	4.00(±0.91)	√		√
	Lack of efficient training of end users	4.10(±0.99)	√		√
	Repayments and insurances	3.95(±1.11)	√		√
	Failure to provide regular IoT rules and programs by governments (e.g., non-compliance with privacy laws or big data management)	4.40(±0.68)	√		√
	Negligence of governments in (i) promoting the best practices and business model of health care; (ii) Transparency in big data management and IoT (iii) research and development budget allocation; (IV) Development of standards (v) Supervision of start-ups and (vi)	4.33(±0.73)	√		√

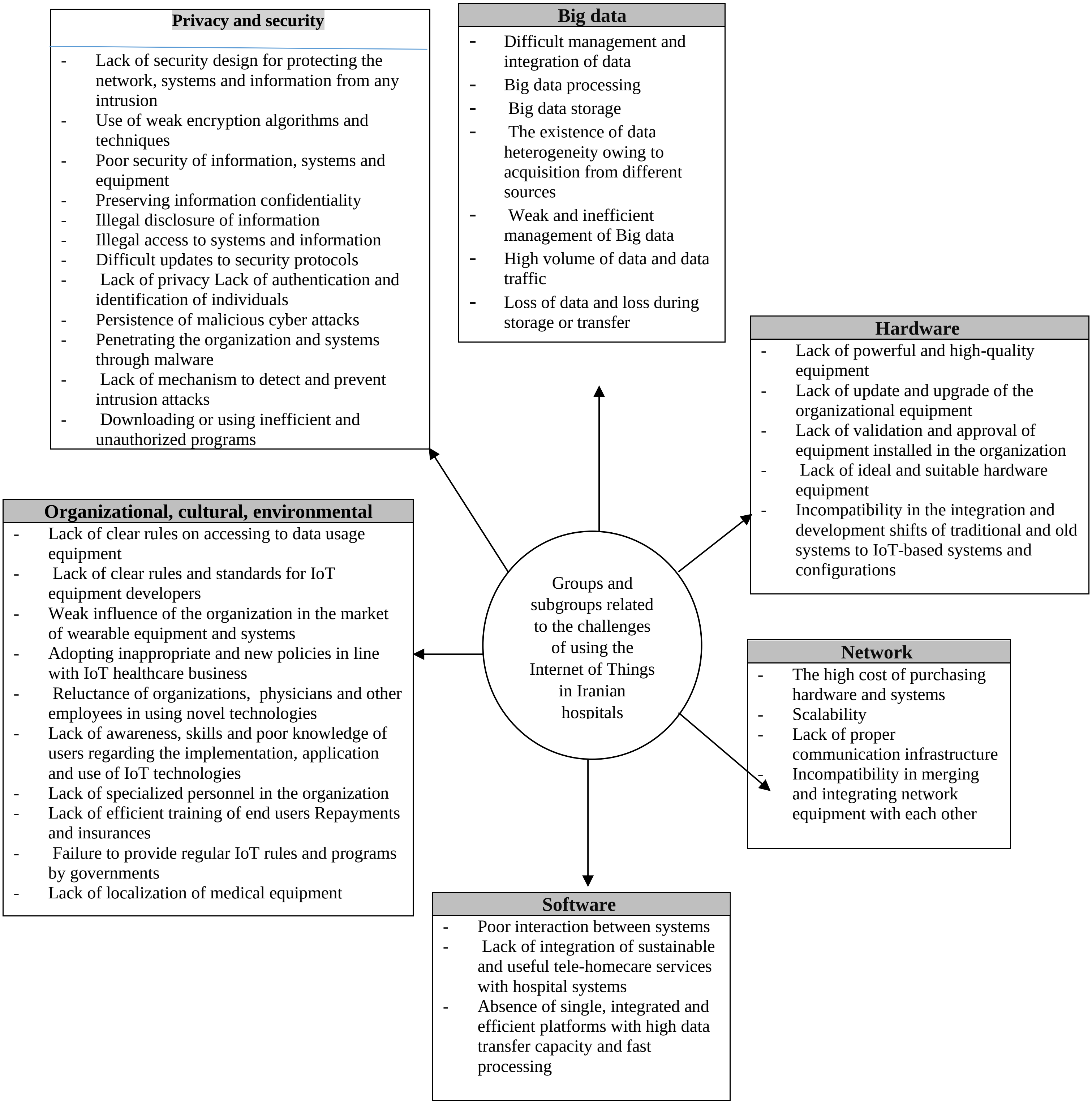
	Training of individuals in various fields of IoT				
	Lack of localization of medical equipment (preparing a product to work in a specific environment)	3.78(±0.99)	√		√
	Failure to use unit standards and protocols for establishing communication between equipment	3.52(±1.07)	*	3.13(±1.12)	×
	Lack of clear rules for the development and use of smart equipment	3.52(±1.07)	*	3.60(±1.24)	×

Note: * Assessment in Second Round of Delphi, ×: Final rejected and √: Final Acceptance

Moreover, in the last part of the questionnaire, i.e. “Other Challenges”, the challenges of lacking enough budget and physical space, communication instruments and protocols (each with a frequency of one) were mentioned by two experts. These challenges were eventually excluded, as the received a mean of less than 50 in the second round of Delphi.

Logical model designed to implement IoT in Iranian hospitals

In the following, the ultimate health system challenges approved for the deployment of the internet of things in Iranian hospitals (Figure 1) and this model is provided based on the above results.



Privacy and security

- Lack of security design for protecting the network, systems and information from any intrusion
- Use of weak encryption algorithms and techniques
- Poor security of information, systems and equipment
- Preserving information confidentiality
- Illegal disclosure of information
- Illegal access to systems and information
- Difficult updates to security protocols
- Lack of privacy Lack of authentication and identification of individuals
- Persistence of malicious cyber attacks
- Penetrating the organization and systems through malware
- Lack of mechanism to detect and prevent intrusion attacks
- Downloading or using inefficient and unauthorized programs

Big data

- Difficult management and integration of data
- Big data processing
- Big data storage
- The existence of data heterogeneity owing to acquisition from different sources
- Weak and inefficient management of Big data
- High volume of data and data traffic
- Loss of data and loss during storage or transfer

Hardware

- Lack of powerful and high-quality equipment
- Lack of update and upgrade of the organizational equipment
- Lack of validation and approval of equipment installed in the organization
- Lack of ideal and suitable hardware equipment
- Incompatibility in the integration and development shifts of traditional and old systems to IoT-based systems and configurations

Organizational, cultural, environmental

- Lack of clear rules on accessing to data usage equipment
- Lack of clear rules and standards for IoT equipment developers
- Weak influence of the organization in the market of wearable equipment and systems
- Adopting inappropriate and new policies in line with IoT healthcare business
- Reluctance of organizations, physicians and other employees in using novel technologies
- Lack of awareness, skills and poor knowledge of users regarding the implementation, application and use of IoT technologies
- Lack of specialized personnel in the organization
- Lack of efficient training of end users Repayments and insurances
- Failure to provide regular IoT rules and programs by governments
- Lack of localization of medical equipment

Groups and subgroups related to the challenges of using the Internet of Things in Iranian hospitals

Network

- The high cost of purchasing hardware and systems
- Scalability
- Lack of proper communication infrastructure
- Incompatibility in merging and integrating network equipment with each other

Software

- Poor interaction between systems
- Lack of integration of sustainable and useful tele-homecare services with hospital systems
- Absence of single, integrated and efficient platforms with high data transfer capacity and fast processing

Figure 1: Final confirmed challenges of using IoT in health systems

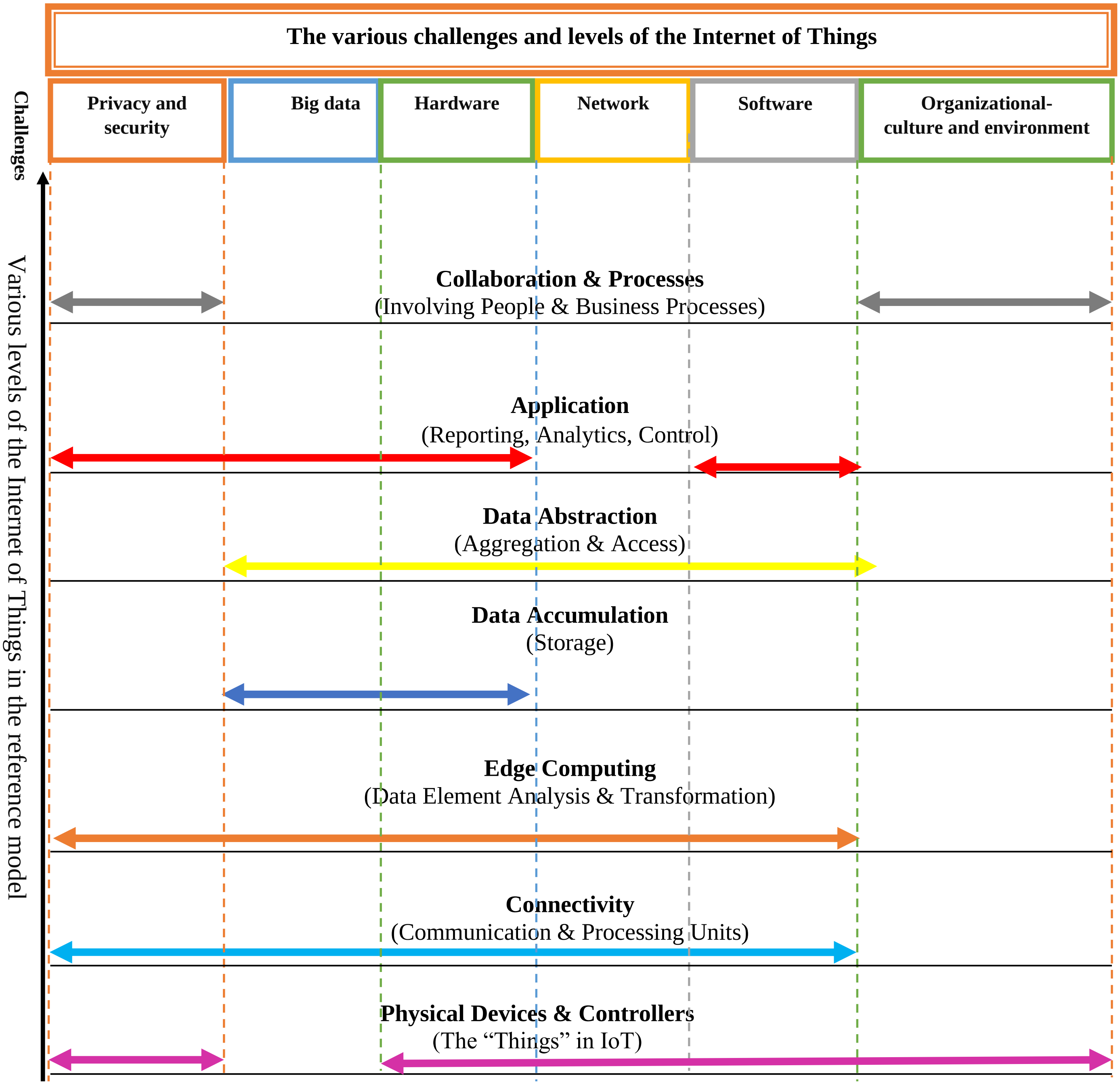

The various challenges and levels of the Internet of Things
Challenges
Privacy and security
Big data
Hardware
Network
Software
Organizational-culture and environment
Various levels of the Internet of Things in the reference model
Collaboration & Processes
(Involving People & Business Processes)
Application
(Reporting, Analytics, Control)
Data Abstraction
(Aggregation & Access)
Data Accumulation
(Storage)
Edge Computing
(Data Element Analysis & Transformation)
Connectivity
(Communication & Processing Units)
Physical Devices & Controllers
(The "Things" in IoT)

Figure 2: A novel model for implementing internet of things in Iranian hospitals

Discussion

In this study, a novel model for implementing Internet of Things (IoT) in Iranian hospitals was designed and presented based on the challenges of using IoT in health systems. This novel model consisted of six main groups, namely privacy and security, big data, hardware, network, software, and organizational-cultural and environmental issues with 78 challenges. From the 78 challenges recognized, 46 were ultimately confirmed by experts as the challenges of using IoT in health systems. Among the groups, organizational-cultural and environmental challenges and privacy and security groups were finally approved by experts as to having the most subgroups. Also, the highest mean in the first round Delphi was assigned to the subgroups of the organizational-cultural and environmental. Moreover, in the second round of Delphi, the subgroups of privacy and security were the most important challenges.

Zubiaga et al. (Zubiaga, Procter, & Maple, 2018) identified the challenges and opportunities of the IoT in their research. They used the Twitter microblogging platform to seek the opinions of skilled professionals regarding IoT. According to their findings, the most negative emotions and main concerns of the participants were associated with security challenges. Although they also used the opinion of experienced people, and similar to the current study, security and privacy challenges were introduced as the most important challenges, but, in this study the challenges were identified in tweets, no categorization was performed on challenges, and no reference model was provided.

Selvaraj et al. (Selvaraj & Sundaravaradhan, 2020) analyzed the latest research articles related to the internet of things healthcare system. Factors such as high energy consumption, fewer available resources, and security issues were recognized as major concerns in the IoT. Through reviewing previous body of literature, Zeadally et al. (Zeadally et al., 2019) introduced dimension of security and privacy, authentication, issues of interactivity, health information exchange, communication between devices, data collection and management, design and implementation based on multidisciplinary knowledge as the most important challenges facing the implementation of IoT. In contrast to the present study, in Selvaraj & Sundaravaradhan and Zeadally et al. no reference model based on challenges was presented in the aforementioned.

Julia et al. (Joyia et al., 2017) outlined the challenges by examining the previous body of literature and without relying on the opinion of experts. Their study presents more challenges compared to our studies, but, no model was proposed for employing the internet of things for healthcare based on these challenges. Cisco Systems, Inc. offered one of the most insightful studies in providing a reference model for using the Internet of Things. They presented a seven-layer reference model for IoT. This reference model is used as the basis for the model presented in this study. However, in contrast the present study, this reference model has not pointed out the underlying challenges, and only the various levels at which the internet of things can be employed in an institution or organization have been outlined.

The issue that should be addressed now is why the challenges of the two dimensions of organizational-cultural and environmental group and privacy and security among the other six groups were recognized by IoT experts of Iran as the most important group in the first and second rounds of Delphi?

Brous et al. (Brous, Janssen, & Herder, 2020) argued that organizational and environmental challenges may either refer to the aspect in which the organization operates or may indicate cultural, social, political, or geographical conditions. Therefore, technologies must be developed or configured as to suit specific environments and meet demands. Kavio et al. (Kaivo-Oja, Virtanen, Jalonen, & Stenvall, 2015) also recognized organizational issues as the foundation for knowledge-based decision-making. Brous et al. (Brous et al., 2020), divided the organizational implications of accepting IoT into structural changes in data management, new responsibilities for monitoring settings, structural changes in policies and processes of provision, structural changes in processes of business conduct, structural changes in strategy and policy, and structural changes in communications. Regarding cultural issues, Aktas et al. (Aktaş, Çiçek, & Kıyak, 2011) outlined that culture affects the decision-making and problem-solving processes, motivation, satisfaction and morale of individuals, and the level of creativity and innovation, and culture and management cannot be conferred separately. Organizational culture grants the members of an organization a sense of identity, through which organizational managers can control employees' work and social ethics and attitudes through unscripted rules, group norms, and the resulting attention.

It is evident from such studies that the dimension related to the organizational-cultural and environmental challenges has been heavily outlined by the experts, and the significance of these challenges has not been overlooked by them. According to the findings of this section, various challenges within organizations affected by organizational-cultural and environmental factors can have both direct and indirect effects on employees' organizational attitudes and thus more importantly the form and rules of employing IoT technology through the challenges of lack of clear rules and standards, poor involvement of organization in the market of wearable equipment and systems, repayments and insurances, and ineffective training of end users among others. Consequently, even though organizational-cultural and environmental issues affecting organizational performances are usually considered very important and negative in this study, according to experts and in many cases may have varying impacts, they should be strictly managed in case of persistence.

Regarding the challenges of IoT privacy, Alkhatib et al. (Alkhatib, Waycott, Buchanan, & Bosua, 2018) argued that there is still no insightful understanding of the concept of privacy in the development community and by focusing on some aspects of privacy while ignoring other important aspects, developers are offering poor outlooks for privacy. Therefore, in the application of the Internet of Things, privacy challenges should be considered as an ever-present fundamental principle and rule. Likewise, security challenges necessitate the ability to ensure security through authentication, confidentiality, ultimate security, and integrity among others (Mahmoud, Yousuf, Aloul, & Zualkernan, 2015). Alkhatib et al., (Alkhatib, Waycott, Buchanan, & Bosua, 2018) noted that by focusing on 13 of the 14 security and privacy challenges, experts have not offered a weak perspective on privacy and are have not dedicated their efforts on just one or a few simple dimensions of security and privacy challenges. Also, according to this study, the challenges of security and privacy has been considered by experts of the field as a basic principle in employing the IoT, and all aspects of guaranteeing security via authentication, confidentiality, security, integrity, etc are covered.

Among the limitations of this study is the lack of similar previous literature in the field of IoT implementation model. As such, since each of the identified challenges can itself be and avenue of research for it researchers, it is recommended that each of such challenges be used separately as a research area for providing an IOT application model. Three databases, IEEE, PubMed and Web of Science, were searched to identify the related studies. Searching in more databases may yield more comprehensive results. The number of experts participating in the first and second stages of Delphi in the present study was 20. More comprehensive results can be attained if a bigger sample size was used in future study. It is also suggested that the proposed model be used to implement several small pilot projects and generalize the results to develop and deploy national-scale projects from the level of the ministry of health to macro-health institutions.

Conclusion

In the present study, a model for implementing the internet of things in Iranian hospitals was proposed based on the challenges of using IoT in health system in six groups of privacy and security, big data, hardware, network, software and organizational-cultural and environmental challenges. This model can provide a sufficient basis; information and knowledge for policymakers, government officials and managers use the internet of things in hospitals of Iran and other regions of the world. Furthermore, this model can fill in the gaps of the challenges of IoT business models, lead to the enhancement of special capabilities in the design of systems, and provide grounds for saving money and time and reduce failure in the initial design of IoT projects.

Since this model of implementing the internet of things in hospitals can develop into practical knowledge and deployment in the real world after thorough interpretation and analysis, another application of this is that it can help the experts in this field to decide regarding the process of implementing large-scale projects in the near future, and when an organization decides to employ IoT technology in a specific area, this study will be considered as a tool to help the faster and more accurate deployment of models in the real world.

Acknowledgments

The authors hereby thank the teaching and research staff of the Non-governmental Electronic Higher Education’s Institute, Faran (Mehr Danesh), as an executor of virtual learning in Iran for supporting this research.

References

Aktaş, E., Çiçek, I., & Kıyak, M. (2011). The effect of organizational culture on organizational efficiency: The moderating role of organizational environment and CEO values. Procedia-Social and Behavioral Sciences, 24, 1560-1573.

Albishi, S., Soh, B., Ullah, A., & Algarni, F. (2017). Challenges and Solutions for Applications and Technologies in the Internet of Things. Procedia Computer Science, 124, 608-614.

Alkhatib, S., Waycott, J., Buchanan, G., & Bosua, R. (2018). Privacy and the Internet of Things (IoT) Monitoring Solutions for Older Adults: A Review. Stud Health Technol Inform, 252, 8-14.

Atlam, H., Walters, R., & Wills, G. (2018). Internet of things: state-of-the-art, challenges, applications, and open issues. International Journal of Intelligent Computing Research (IJICR), 9(3), 928-938.

Bakhshi, Z., Balador, A., & Mustafa, J. (2018). Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models. Paper presented at the 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW).

Brous, P., Janssen, M., & Herder, P. (2020). The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. International Journal of Information Management, 51, 101952.

Faber-Wildeboer, A. T., van Os-Medendorp, H., Kooy, A., & Sol-De Rijk, B. (2013). Prevalence and risk factors of depression and diabetes-related emotional distress in patients with type 2 diabetes: A cross-sectional study. Journal of Nursing Education and Practice, 3(6), 61.

Gia, T. N., Rahmani, A.-M., Westerlund, T., Liljeberg, P., & Tenhunen, H. (2015). Fault tolerant and scalable IoT-based architecture for health monitoring. Paper presented at the 2015 IEEE Sensors Applications Symposium (SAS).

Hsu, C.-C., & Sandford, B. A. (2007). The Delphi technique: making sense of consensus. Practical Assessment, Research, and Evaluation, 12(1), 10.

Hussein, A. (2019). Internet of Things (IOT): Research Challenges and Future Applications. IJACSA) International Journal of Advanced Computer Science and Applications, 10(6), 77-82.

Ifrim, C., Pintilie, A.-M., Apostol, E., Dobre, C., & Pop, F. (2017). The Art of Advanced Healthcare Applications in Big Data and IoT Systems. In (Vol. 22, pp. 133-149).

Joyia, G. J., Liaqat, R. M., Farooq, A., & Rehman, S. (2017). Internet of Medical Things (IOMT): applications, benefits and future challenges in healthcare domain. J Commun, 12(4), 240-247.

Kaivo-Oja, J., Virtanen, P., Jalonen, H., & Stenvall, J. (2015). The effects of the internet of things and big data to organizations and their knowledge management practices. Paper presented at the International Conference on Knowledge Management in Organizations.

Kisa, S. (2008). Turkish nurses' concerns about home health care in Turkey. Australian Journal of Advanced Nursing, The, 25(4), 97.

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures. Paper presented at the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST).

Modarresi, A., Gangadhar, S., & Sterbenz, J. P. (2017). A framework for improving network resilience using SDN and fog nodes. Paper presented at the 2017 9th International Workshop on Resilient Networks Design and Modeling (RNDM).

Moulaei, K., Malek, M., & Sheikhtaheri, A. (2019). Monitoring of external predisposing factors for Diabetic Foot: A literature review and physicians' perspectives. Medical Journal of the Islamic Republic of Iran, 33, 159-159. doi:10.34171/mjiri.33.159

Moulaei, K., Bahaadinbeigy, K., & Fatehi, F. J. C. D. (2021). A novel minimum data set (MDS) for the management of diabetic foot: basis for introducing effective indicators to the better management, control and monitoring of diabetic foot. Clinical Diabetology, 2021.

Rghioui, A., & Oumnad, A. (2018). Challenges and opportunities of internet of things in healthcare. International Journal of Electrical and Computer Engineering, 8(5), 2753.

Selvaraj, S., & Sundaravaradhan, S. (2020). Challenges and opportunities in IoT healthcare systems: a systematic review. SN Applied Sciences, 2(1), 139.

Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and challenges for realising the Internet of Things. Cluster of European Research Projects on the Internet of Things, European Commision, 3(3), 34-36.

T. Devendran, D. A. A. A., S.Suseela. (2018). Challenges And Issues Of Healthcare In Internet Of Things (Iot) International Journal of Latest Trends in Engineering and Technology, 2018(Special Issue), 86-091.

Tracking the Internet of Things for the Australian IT community

(2020, 2018). Tracking the Internet of Things for the Australian IT community. Retrieved from https://www.iotaustralia.org.au/2015/07/22/iotnewsglobal/cisco-iot-world-forum-reference-model-promises-interoperability/

Upadhyay, S. (2018). Ongoing Challenges and Research Opportunities Internet Of Things(IOT). International Journal of Engineering Technologies and Management Research, 5(2), 216-222.

Weyrich, M., & Ebert, C. (2015). Reference architectures for the internet of things. IEEE Software, 33(1), 112-116.

Zeadally, S., Siddiqui, F., Baig, Z., & Ibrahim, A. (2019). Smart healthcare: Challenges and potential solutions using internet of things (IoT) and big data analytics. PSU research review, 1-17.

Zubiaga, A., Procter, R., & Maple, C. (2018). A longitudinal analysis of the public perception of the opportunities and challenges of the Internet of Things. PloS one, 13(12), e0209472-e0209472. doi:10.1371/journal.pone.0209472