Technology in Society xxx (2018) 1–11

Contents lists available at ScienceDirect

Technology in Society

journal homepage: www.elsevier.com/locate/techsoc

A Fuzzy Analytic Network Process (FANP) approach for prioritizing internet of things challenges in Iran

Ali Kamali Mohammadzadeh [a], Saeed Ghafoori [a], Ayoub Mohammadian [b], Reza Mohammadkazemi [c], Bahareh Mahbanooei [d], Rohollah Ghasemi [e], *

[a] *Faculty of Management, University of Tehran, Hasan Abad-e-Baqerof, Jalal ale ahmad Highway, Chamran, Tehran, 14117-13114, Iran*
[b] *Assistant Professor of Information Technology (IT) Management at University of Tehran, Hasan Abad-e-Baqerof, Jalal ale ahmad Highway, Chamran, Tehran, 14117-13114, Iran*
[c] *Associate Professor in Management and Planning Faculty of Entrepreneurship, Department of Business, University of Tehran, Farshi Moghadam (16 St.), North Kargar Ave., Tehran, 14398-143141, Iran*
[d] *Ph.D. Candidate in Organizational Behavior Management at University of Tehran, Old Qom-Tehran Road, College of Farabi, University of Tehran, Qom, 37181-17469, Iran*
[e] *Ph.D. in Production and Operations Management, Hasan Abad-e-Baqerof, Jalal ale ahmad Highway, Chamran, Tehran, 1411713114, Iran*

ARTICLE INFO

Article history:
Received 12 August 2017
Received in revised form
1 January 2018
Accepted 17 January 2018
Available online xxx

Keywords:
Internet of Things (IoT)
Technology development challenges
Fuzzy analytic network process (FANP)

ABSTRACT

Recent years have witnessed a huge upsurge of interest in internet of things (IoT) throughout the world. This shift has led to the emergence of new challenges associated with this novel paradigm. They all need to be addressed properly by experts and scholars in the field.

In this paper, an integrated approach using fuzzy analytic network process (FANP) was applied to carry out the following tasks: first, to identify the most important IoT technology development challenges in Iran and secondly, to prioritize the aforementioned factors.

The implemented approach took into account that technological factors, privacy and security issues, business related factors, legal and regulatory challenges, and cultural elements are the main factors which have an impact on IoT technology development. Besides, it was also taken into consideration that several correlations among the aforementioned classes exist.

The results indicate that “technological” and “privacy and security” challenges are the most significant factors which affect IoT. Furthermore, “business model”, “architecture and design” and “education and training” were ranked as the most considerable sub-factors respectively.

1. Introduction

Innovation-driven economies have depicted the value of innovation in Business Ecosystem vividly. The role of technology in the advent of innovation has been one of the most challenging debates of our generation. In order to increase social welfare, economic prosperity and environmental care, new technologies can play a significant role in sustainable development. Besides, Due to eradication of non-effective processes and reallocation of resources, new technologies increase the effectiveness of measures that will lead to the development of innovation. Therefore, countries should improve their competitiveness through transition from Factor-driven economy toward Efficiency-driven economy and eventually to an innovative one.

According to global competitiveness index (GCI), Iran, as a transition country from a factor-based economy to an efficiency-driven one [3,4], is seeking to improve its competitiveness status. One of the pillars of competitiveness, with regard to new technologies, is technological readiness. Thus, to enhance the global competitiveness, accurate strategic planning should be taken into serious consideration. On the other hand, the results of these efforts will be ascertained in the long run. Hence, focusing on emerging technologies, which are expected to have a significant contribution in the competitiveness in the future, is a necessity for policy making. According to Gartner's report in 2015, the Internet of Things (IoT) is among the technologies that are expected to reach “Peak of

* Corresponding author.
E-mail addresses: Alikamali@ut.ac.ir (A.K. Mohammadzadeh), Saeedghafoori@ut.ac.ir (S. Ghafoori), mohamadian@ut.ac.ir (A. Mohammadian), r_mkazemi@ut.ac.ir (R. Mohammadkazemi), b.mahbanooi@ut.ac.ir (B. Mahbanooei), ghasemir@ut.ac.ir (R. Ghasemi).

https://doi.org/10.1016/j.techsoc.2018.01.007
0160-791X/© 2018 Published by Elsevier Ltd.

Inflated Expectations” in the upcoming decade. IoT is one of the forefront technologies that many countries have been invested on as their future innovation driver [5,6]. To this end, the first step is to identify the IoT technology development challenges. However, The challenges in this area have rarely investigated in developing countries and the knowledge is limited [7,8].

Iran, as a developing country, has shown increasing interest in IoT and has undertaken some noteworthy efforts in Iran Telecommunication Research Center (ITRC) based on its 1404 outlook. Among these efforts “Internet of Things (IoT) Research, Market and Industries” project can be mentioned [4].

As the responsible institute for IoT technology development, ITRC investigated IoT in terms of governance, technology, market, network, security, and usability. Based on these investigations, it can be claimed that the importance of the Internet of Things is still misunderstood in Iran and IoT applications in Iran is limited to Machine to Machine (M2M) communication and Radio-frequency Identification (RFID) technology development. Ergo, this paper aims to increase IoT development knowledge through investigating its challenges on one hand, and provide practical solutions, as executive strategies, for policymakers through prioritizing the aforementioned challenges on the other hand. Thus, the questions which this study aims to address are as follows:

1. What are the IoT technology development challenges (in Iran)?
2. How is the prioritization of the aforementioned challenges (in Iran)?

The rest of the paper is structured as follows. Section 2 reviews the background and highlights the most important challenges IoT technology development is faced with. Section 3 describes the research methodology. Section 4 discusses the experimental results and discussion. Finally, section 5 concludes the paper.

2. Literature review

The term Internet of Things is a novel paradigm that is in rapid progress in the area of wireless telecommunications [9]. Although there is no single, global definition, the fundamental idea of this concept is the ubiquitous presence of a variety of things or objects which are able to generate, exchange and consume data with minimal human intervention to reach common goals [10,11].

Most of the studies in the field of system development, technology development, and internet of things, addressed the challenges along with the identification of barriers, opportunities, and many of which did not prioritize challenges [12–14]. Al-Mabrouk addressed the concerns about technology transfer [15]. Azad examined the challenges of the business model in IoT [16]. Mousa addressed E-government challenges in the UK [17]. Park considered the vital security requirements of IoT [18]. Syamsuddin evaluated E-government security strategies [19]. However, a comprehensive study on the identification of IoT challenges was not found. Nevertheless, addressing all the challenges IoT faces and prioritizing them seems absolutely necessary.

In a number of reviewed studies, prioritizing specific domains of technology or IoT challenges were undertaken. Methodologically speaking, three general categories were observed in these studies. In the first class, strategic planning methods have been utilized. Among these studies [20], can be mentioned. The second group used qualitative techniques for prioritizing. Among these studies [15], used the Delphi methodology and [17] conducted semi-structured interviews. Finally, the third category of studies has used multi criteria decision making (MCDM) techniques for prioritizing. To enumerate some [16], combined fuzzy DEMATEL and ANP [18], implemented FANP and fuzzy DEMATEL and [19] utilized FAHP.

It would be almost impossible to cover the extensive range of challenges surrounding IoT in a single paper. In this paper, however, after reviewing the literature, IoT technology development challenges were identified in the relevant scientific literature. Afterwards, the challenges were categorized in 5 distinct categories in a hierarchical structure and then presented to the expert team. The expert team evaluated and confirmed the aforementioned challenges and the presented structure as well. Afterwards, the adequacy of the identified challenges was confirmed by the expert team and the validity of the questionnaire was verified.

As mentioned, this article provides an overview of five distinct classes regarding IoT including: Security and privacy challenges, legal and regulatory challenges, technological challenges, cultural challenges and business challenges which will be discussed in the following.

2.1. Security and privacy challenges

Due to the vast scale of IoT based networks, security and privacy challenges of IoT have become more salient compared with other state of the art technologies [21]. These issues are at the heart of trust, relationship building, and different forms of exchange [22] and negligence in meeting them appropriately may have crucial consequences such as causing damage, disruption to operations or even loss of life [23].

While some researches considered security and privacy as two distinct categories [14], they are being considered as one single category in other investigations [24]. Due to their significant overlap and their mutual impact over each other, this paper adopts the latter approach. The most prominent challenges regarding security and privacy include: Transparency, conflict of interests, data confidentiality, network security and IoT devices' safety.

2.1.1. Transparency

A large number of IoT devices function in a way that the user has little or no awareness of their precise operations. This leads to a security vulnerability when an IoT device might be performing undesirable functions or collecting data that the individual does not intend [25]. Besides, the alterations of the device's function through updates should not be neglected. These challenges have a quiddity of security and privacy simultaneously. Finding the degree of transparency which enforces the user's privacy preferences is a non-negligible challenge in the context of security and privacy.

2.1.2. Conflict of interests

The expectations of privacy differ in public and private sectors and IoT challenges these differences [25]. Many IoT devices perform in situations in which multiple people are subject to the same data collection activity. Location tracking systems and surveillance cameras are two examples of such situations. In these situations it might be difficult or even impossible to distinguish, individual privacy preferences [25]. The conflict of interest does not occur merely amongst users. Different expectations, demands and perceptions among manufacturers and users, government and citizens (e.g. surveillance cameras), or government and manufacturers may give rise to a diverse range of conflicts.

2.1.3. Data confidentiality

The IoT devices collect and store a tremendous amount of information. Ergo, they carry a significant potential of privacy risks with respect to the use of the data and its accessibility [26]. In order to ensure security of data, services and the entire IoT system, confidentiality of the collected data must be guaranteed [27]. Due to the environmental characteristics of IoT and the devices' heterogeneity, this is an extremely challenging issue.

2.1.4. Network security

The term network security refers to the mechanisms exerted within a network in order to ensure trusted operation of the IoT [28]. Security is absolutely essential to any network [29] and since extant security architecture is designed from human communication perspective, it may not be suitable for IoT system [30]. Hence, it is of high importance to develop reliable strategies to ensure the security of the IoT network.

2.1.5. IoT devices' safety

Plenty of IoT devices has not been developed with security in mind. A multitude of them contain embedded softwares which are troublesome to patch and upgrade, which leads to vulnerability and configuration management issues. According to SANS, merely 52 percent of IoT devices undergo security tests prior to production [23]. Besides, a recent research undertaken by HP Fortify found that the average security concerns per device is equal to 25 and 70 percent of the most generally used IoT devices are prone to security vulnerabilities [23].

2.2. Legal and regulatory challenges

The advent of IoT has raised a broad range of questions and challenges from a legal and regulatory perspective, which need thoughtful deliberation. In some scenarios, IoT engenders new legal and regulatory concerns that did not exist hitherto. It also amplifies a plethora of extant issues in many other cases [25]. A number of potential legal and regulatory challenges are discussed below.

2.2.1. Cross boarder data flows and global cooperation

The span of IoT is not restricted to just one jurisdictional boundary. It is possible for IoT devices to collect data in one jurisdiction and transfer it to another jurisdiction for storage or processing [25]. This feature can pose a potential challenge when the Laws and regulations are inconsistent or incompatible amongst the jurisdictions. Besides, due to the lack of a single, universal approach toward IoT Legislation, the challenge of cooperation amongst beneficiary countries would be intensified.

2.2.2. Data usage

IoT devices learn about consumers' habits, preferences and purchasing behavior through web-related data [22]. There are, however, some concerns with regard to the way this data is being utilized. Discriminatory use of data, using data in order to enforce the law and normative uncertainty [26] are just three examples of the challenges which should be overcome by means of appropriate legislation.

2.2.3. Liability

IoT devices pose considerable legal liability challenges that need careful deliberation [25]. The most primary question regarding IoT devices' liability is “who is responsible If someone is injured due to an IoT device's operation?”. IoT devices operate in a way more complex manner than a traditional products, which will lead to more complicated scenarios.

2.2.4. Ownership (intellectual property)

The issue of ownership has been also a matter of concern. In a system where a multitude of parties adds value, who owns the data? [22].

2.2.5. Standardization

The standardization of IoT includes the architecture standards, the application requirements standards, the communication protocol standards, the identification standards, the security standards, the application standards, the data standards, the information processing standards, and the public service platform standards [30]. In order to prevent anarchy in the IoT world, it is necessary to enhance the standardization of applications [5].

2.3. Technological challenges

IoT embraces an extremely wide range of technologies. These technologies can be intricate for a variety of reasons and hence may introduce problems and hinders development of IoT and eventually block it from connecting as many “Things” as possible [30].

2.3.1. Architecture and design

Designing a Secure, flexible and cost-efficient architecture is of paramount importance for IoT fast adoption. A plethora of solutions have been proposed in recent years. The majority of them have been from the wireless sensor networks (WSN) perspective [29,31], while some have been from different standpoints [29]. Nevertheless, the issue is still open to debate.

2.3.2. Addressing

The IoT includes an extremely vast number of nodes which produce massive content that should be accessible by authorized users regardless of their position. This necessitates effective addressing policies [9,32].

Addressing refers to the mechanism of identifying objects within a network [33]. Although a lot of approaches toward addressing have been proposed, opting a unique solution is exceedingly challenging due to heterogeneity of the identifier lengths used by various technologies [34].

2.3.3. Devices heterogeneity (managing heterogeneity)

Based on Gartner's report, the present architecture of IoT is not prepared to cope with the heterogeneous nature of personal and enterprise data [35]. Different applications and environments need distinct networking technologies, and the range of technologies are significantly divergent from each other [36]. This compromises the IoT user' ability to connect and share which is fundamental to development of IoT [25]. Managing this incongruity is still an open challenge.

2.3.4. Ubiquitous data management

IoT devices generate a tremendous amounts of data that should be processed and stored [37]. As IoT devices become more prevalent, managing this volume of data will become more challenging to address adequately [5]. Besides, the data obtained from IoT devices need to be processed and analyzed using computers and mathematical models. Considering the enormous amount of data, which is not processable using traditional data mining techniques, there is a shortage of advanced data mining tools and competent data analysts [38]. Furthermore, transmitting data from one jurisdictional boundary to another should not be neglected. It should be noted that this particular form of ubiquitous data exchange may raise not only technological, but also legal challenges [25].

2.3.5. Hardware construction

Hardware design refers to a system's tangible components and their interactions. It not only affects the efficiency and effectiveness of the IoT, but also has a significant impact on issues such as the energy consumption and management, disposal of devices and environmental pollution [39].

2.3.6. *Fault tolerance*

In a hyper-connected world, a minor malfunction in one part of a system may lead to catastrophic consequences. Besides, heterogeneous networks provide more than just one distinguished service or application. These two statements imply the exigency of a single network to support all applications without deficiency. It is an arduous task to provide guarantees in wireless networks. Considering the proliferating number of poorly tested devices, inattention to this challenge may turn our lives into chaos [5].

2.4. *Cultural challenges*

2.4.1. *Education and training*

It is not possible to make the most of IoT's potential without adequate education and training. As governments and organizations must learn to use the IoT platform properly and effectively, people must also acquire knowledge and skill of utilizing its features appropriately [25].

2.4.2. *Vandalism*

Many IoT devices are vulnerable to vandalism. Regardless of being intentional or unintentional, IoT devices should be utilized in a way that minimizes damage from vandalism. Designing resistant to vandalism devices, installing them without being too conspicuous and locating the devices in secure places are among possible solution Which can be considered by IoT security professionals [40].

2.4.3. *Trust*

Ensuring trust in the IoT is of significant importance and impacts the ability of individuals to connect, communicate and share in meaningful ways. If efforts to create trust in IoT fails, rapid development of IoT would not be possible [41].

2.4.4. *Ethics*

IoT devices have designed to collect and store data about their environment, which frequently includes data associated with people. Whenever the individuals who are observed have different privacy expectations concerning the use of that data than those of the data gatherer, ethical challenge arises [25].

2.5. *Business challenges*

In the hyper-connected IoT world, businesses should make every effort to palliate the problems and concerns of IoT users as much as possible. In order to do so, they should move toward new processes and innovative business models [42,43].

2.5.1. *Economic development opportunities and issues*

According to McKinsey Global Institute, IoT has remarkable potential in developing economies. This potential can ameliorate global issues such as sustainable agriculture, energy consumption, water availability, and management of resources, among others [25]. However, to ensure that the aforementioned benefits are global, some specific issues such as infrastructure resources, investment, industry development and policy and regulatory coordination must be considered.

2.5.2. *Investing in IoT development*

Three approaches are recognizable regarding investment in the IoT. Comprehensive investments in infrastructure, smart cities, software, applications and services, a stakeholder approach that advocates public-private partnerships and vertical investments and an opportunity investment approach that is inspired by short to mid-term return on investment [42]. Each one of these approaches is dominant within a specific region. Alignment of these heterogeneous perspectives would not be possible effortlessly.

2.5.3. *Business model*

There are too many possibilities, uncertainties and concerns in business models in IoT [30]. The advent of new currencies, user lock-in and adopting a universal gateway are among these concerns and uncertainties [44].

2.5.4. *Customer expectations and quality of service*

In the current era, customer expectations are constantly rising. Fulfilling the customers' needs, expectations and preferences is the only way to ensure their loyalty and the any given organization's survival and growth. IoT provides an excellent platform to do so. There are, however, plenty of challenges to meet. Among them choosing the proper technology to create preferable experiences, designing appropriate customer feedback process and understanding customer needs and expectations and knowing how to meet them could be mentioned [45–48].

2.6. *Proposed model for IoT challenges*

In this paper, IoT Challenges were divided into five categories: Privacy and security challenges, Legal and regulatory challenges, Technological challenges, Cultural challenges and Business challenges. Each category contains a number of challenges which is shown is the Fig. 1. In Table 2 some of the papers which have referred these challenges are mentioned.

3. Research methodology

3.1. *Analytic network process (ANP)*

Built on the Analytic Hierarchy Process (AHP), Saati proposed the ANP in the 1980s and it has been widely used for multi-criteria decision making problems since [49]. Without assuming the independence of elements, the ANP goes far beyond the AHP. Besides, the ANP prioritizes not just elements, but also clusters or sets of elements as is frequently essential in the real world problems [50].

The process of ANP consist of 3 steps as follows [51]:

Step 1: The decision-makers evaluate all proposed criteria pairwise without considering the interdependence among them. The responses are presented numerically on the basis of Saaty's scale. Each pair must be judged only once. A reciprocal value will be assigned to the reverse comparison automatically. After completing the pairwise comparisons, the local weight vector w_1 is calculated as the unique solution to

$$\mathbf{A}\, w_1 = \lambda_{\max}\, w_1$$

where $\lambda_{\max}$ is the largest eigenvalue of pairwise comparison matrix **A**. The resulting vector is normalized by dividing each value by its column total to represent the normalized local weight vector w_2.

Step 2: In this step, interdependence between the evaluation criteria is to be computed. The decision-makers evaluate the impact of the criteria on each other using pairwise comparisons just like step 1. Subsequently, for each criterion, a pairwise comparison matrices is formed. The normalized eigenvectors for the aforementioned matrices are computed in interdependence weight matrix of criteria **B**.

Step 3: In this step, by combining the results from previous steps, the interdependence weights of the criteria can be obtained as follows:

$$w_c = \mathbf{B} w^{\mathrm{T}}{}_{2.}$$

Please cite this article in press as: A.K. Mohammadzadeh, et al., A Fuzzy Analytic Network Process (FANP) approach for prioritizing internet of things challenges in Iran, Technology in Society (2018), https://doi.org/10.1016/j.techsoc.2018.01.007

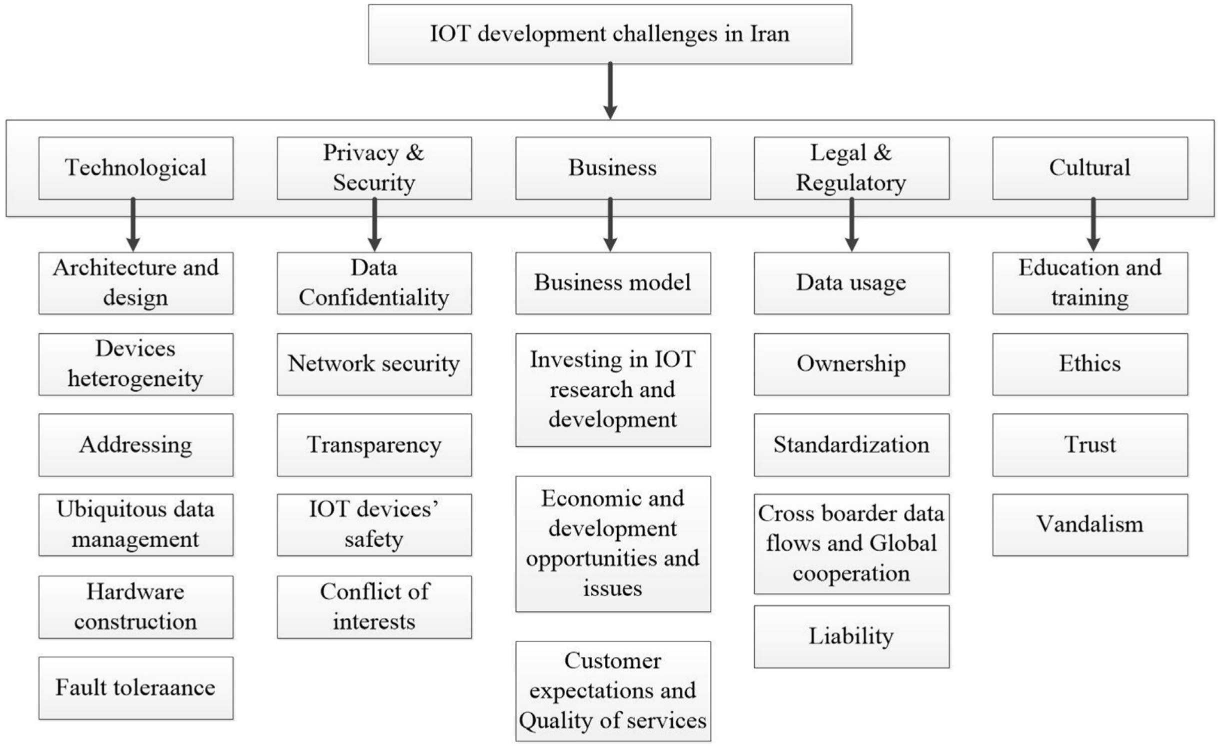

Fig. 1. IoT technology development challenges hierarchical structure.

Table 1
Stages of economic growth.

Stages of economic growth	Definition	Example
Factor-driven economy	Countries' growth is based on the unskilled labor and natural resources and companies compete on the basis of price [1].	India, Russia, Iran [2]
Efficiency-driven economy	Countries' growth is based on the efficient production processes and companies compete on the basis of quality [1].	Brazil, China [2],
Innovation-driven economy	Countries' growth is based on the new and different products and services and companies compete on the most sophisticated process [1].	Qatar, Canada Australia [2],

Table 2
The identified factors and sub-factors.

Factors	Sub-factors	Reference
Technological	Architecture and design	[31]
	Devices heterogeneity	[36]
	Addressing	[9]
	Ubiquitous data management	[5]
	Hardware construction	[39]
	Fault tolerance	[5]
Privacy and security	Data confidentiality	[26]
	Network security	[29]
	Transparency	[25]
	IoT devices' safety	[23]
	Conflict of interests	[25]
Business	Business model	[44]
	Investing in IoT development	[42]
	Economic development opportunities and issues	[25]
	Customer expectations and Quality of service	[45]
Legal and regulatory	Data usage	[22]
	Ownership	[22]
	Standardization	[30]
	Cross boarder data flows and Global cooperation	[25]
	Liability	[25]
Cultural	Education and training	[25]
	Ethics	[41]
	Trust	[40]
	Vandalism	[40]

Please cite this article in press as: A.K. Mohammadzadeh, et al., A Fuzzy Analytic Network Process (FANP) approach for prioritizing internet of things challenges in Iran, Technology in Society (2018), https://doi.org/10.1016/j.techsoc.2018.01.007

Evaluating alternatives always contain ambiguity and plurality of meaning. Besides, in case of qualitative attributes, human assessment is subjective and hence imprecise [52]. Thus, the conventional ANP appears insufficient. In such cases, the fuzzy sets are extremely advantageous and allow a more exact delineation of the decision making process.

Devised to characterize the imprecision or ambiguity of human cognitive processes in a mathematical sense, fuzzy set theory was introduced by Zadeh in the 1960s [53]. Fuzzy set theory has been applied to a vast variety of applications in diverse fields [54–56]. Implementation of fuzzy logic provides to get more reliable judgments of the decision makers than the crisp-based methods.

Due to its applicability in real-world problems, a copious number of fuzzy ANP (FANP) approaches have been proposed in recent years. For instance [57], presented an evaluation approach using a fuzzy ANP for multi-criteria evaluation of contaminated site remedial countermeasures. In another study, Dargi et al. developed a FANP framework for the supplier selection process in automotive industry [58]. For more examples, see Refs. [59–61].

Among all the FANP approaches, Mikhailov's model was chosen for this paper due to its ability to calculate the consistency Index and maximize it as well [62]. The consistency index can determine the reliability of the respective questionnaire and thus can be useful in confirming the reliability of the collected data. Mikhailov asserts that values greater than 0 indicate compatibility in fuzzy judgments. On the other hand, values less than 0 (negative values) account for strong inconsistency. Hence, the compatibility rate between 0 and 1 shows the compatibility of fuzzy comparisons, and the closer it is to 1, the greater the compatibility of judgments are [62].

In this study, triangular fuzzy numbers are used. A triangular fuzzy number (TFN) is denoted as (l,m,u). The parameters l, m and u indicate the smallest possible value, the most promising value, and the largest possible value that describe a fuzzy event, respectively [63].

3.2. Snowball sampling method

Snowball sampling, or chain referral sampling, is a sampling technique where primary subjects recruit future study subjects among their acquaintances. This technique can be used to identify experts in a certain field. Locating hidden population and low cost can be mentioned as snowball sampling method advantages. Snowball sampling starts with a convenience sample of initial subject [64]. The initial subject serve as “seeds,” through which the sample consequently expands through several steps just like a snowball growing in size as it rolls down a hill [65].

In this study, starting snowball sample included 3 IoT experts with at least 3 years of experience in the field of IoT in ITRC which eventually, after implementing snowball sampling technique, led to an expert team of 8 members. The identified group among with the experts in the focus group validated the identified challenges. Subsequently, the focus group evaluated IoT technology development challenges in Iran and the FANP questionnaires were completed.

3.3. Questionnaire design

The design of the questionnaires was carried out according to the model used in this research, presented by Mikhailov [62]. In order to make pair-wise comparisons by the experts, the scale provided in Table 3 was used. For instance, the challenges identified in the “security and privacy” factor, were compared using the question “How important is “transparency” in comparison with “conflict of interests”?" and the respective response, equally important (EI), was placed in the corresponding position in the pair-wise comparison matrix as a triangular fuzzy number (1/2, 1, 3/2).

Here are three important points to consider. First, using a pre-approved questionnaire can help validate the questionnaire. Second, Saati considers homogeneity and clustering as a guarantee for validity insurance [66]. Finally, after confirming each questionnaire, a number of experts reconfirmed its validity and then the questionnaire was distributed among all the experts.

3.4. Methodology

In this study, a fuzzy ANP-based methodology is used to prioritize the IoT development challenges in Iran. This approach is utilized due to its ability in considering more generalized relations than AHP. Furthermore, its combination with fuzzy theory is due to inability of the original ANP model to handle the imprecision and subjectivity in the pair wise comparison process made by the experts and decision-makers. The applied model for prioritizing the IoT development challenges is a five step procedure which is described in detail, below [51]:

1. Employing snowball sampling method, which was explained in section 3.2, opt the IoT experts to identify and categorize the factors and sub-factors.
2. Construct the ANP model's hierarchy which consist of goal, factors and sub-factors.
3. Using pairwise comparison matrices, determine the local weights of the factors and sub-factors. The fuzzy scale regarding relative importance to calculate the relative weights, introduced in 2006 [67], is specified in Table 3. Using the Formula (1), the local weights of the factors and sub-factors are calculated:

$$
\begin{aligned}
& \qquad Max\ \alpha \\
St: & \\
& \qquad\qquad (m_{ij}-l_{ij})\alpha w_j - w_i + l_{ij}w_j \le 0 \\
& \qquad\qquad (u_{ij}-m_{ij})\alpha w_j + w_i - u_{ij}w_j \le 0 \\
& \qquad\qquad \sum_{k=1}^{n} w_k = 1,\ w_k > 0,\ k = 1,\ 2,\ \ldots,\ n \\
& \qquad\qquad i = 1,\ 2,\ \ldots,\ n-1, \quad j = 2,\ 3,\ \ldots n \quad j > i
\end{aligned}
\tag{1}
$$

where w denotes the local weight vector.

The optimal value to the Formula (1) as a non-linear problem, if positive, specifies that all solution ratios completely satisfy the fuzzy judgment. This means that the primary set of fuzzy judgments is rather consistent. A negative value of α^* indicates that the solutions ratios approximately satisfy all double-side inequalities which means that the fuzzy judgments are significantly inconsistent.

4. In this step the interdependent weights of the factors is calculated. Using fuzzy scale, the inner dependence matrix of each factor in connection with the other factors should be determined. Based on the dependencies, dependence among all factors can be defined. The interdependent weights of the factors is equal to the product of the local weights of the factors and inner dependence matrix.
5. The global weights for the sub-factors is determined in this step. By multiplying local weight of the sub-factor, which was calculated in step 3, with the interdependent weights of the relevant factor, which was calculated in step 4, the global weights for the sub-factors is calculated.

4. Experimental results and discussion

The case study for the application of utilized model is “IoT

Table 3
Linguistic scales for difficulty and importance.

Linguistic scale for difficulty	Linguistic scale for importance	Triangular fuzzy scale	Triangular fuzzy reciprocal scale
Just equal	Just equal	(1,1,1)	(1,1,1)
Equally difficult (ED)	Equally important (EI)	(1/2,1,3/2)	(2/3,1,2)
Weakly more difficult (WMD)	Weakly more important (WMI)	(1,3/2,2)	(1/2,2/3,1)
Strongly more difficult (SMD)	Strongly more important (SMI)	(3/2,2,5/2)	(2/5,1/2,2/3)
Very strongly more difficult (VSMD)	Very strongly more important (VSMI)	(2,5/2,3)	(1/3,2/5,1/2)
Absolutely more difficult (AMD)	Absolutely more important (AMI)	(5/2,3,7/2)	(2/7,1/3,2/5)

technology development challenges” in Iran. The factors and sub-factors to be used in the model were determined by the expert team. Pairwise comparison matrices used to calculate factor and sub-factor weights were also formed by the same team. The application performed based on the steps provided in previous section and explained step by step together with the results.

Step 1: In this step the factors and sub-factors are determined as presented in Table 2.

Step 2: In this step the ANP is formed. See Fig. 1.

Step 3: In this step, local weights of the factors and sub-factors are calculated. The ANP questionnaire was presented to the expert team and was completed by them using the scale proposed by Kahraman et al. in Ref. [67]. The results are given in Table 4, Table 5, Table 6, Table 7, Table 8 and Table 9.

Step 4: In this step, interdependent weights of the factors are calculated (Fig. 2).

$$W_{factors} = \begin{bmatrix} Tech \\ Privacy \\ Legal \\ Business \\ Cultural \end{bmatrix} = \begin{bmatrix} 0.75 & 0.1 & 0.2 & 0.10 & 0.15 \\ 0.1 & 0.6 & 0.2 & 0.05 & 0 \\ 0.15 & 0.1 & 0.6 & 0.05 & 0 \\ 0 & 0.15 & 0 & 0.75 & 0 \\ 0 & 0.05 & 0 & 0.05 & 0.85 \end{bmatrix} \times \begin{bmatrix} 0.24 \\ 0.22 \\ 0.18 \\ 0.20 \\ 0.16 \end{bmatrix} = \begin{bmatrix} 0.282 \\ 0.202 \\ 0.176 \\ 0.183 \\ 0.157 \end{bmatrix}$$

Step 5: Using interdependent weights of the factors and local weights sub-factors, global weights for the sub-factors are calculated in this step.

$$W_{Tech\ sub-factors} = \begin{bmatrix} T_1 \\ T_2 \\ T_3 \\ T_4 \\ T_5 \\ T_6 \end{bmatrix} = 0.282 \times \begin{bmatrix} 0.15 \\ 0.15 \\ 0.17 \\ 0.19 \\ 0.17 \\ 0.17 \end{bmatrix} = \begin{bmatrix} 0.0423 \\ 0.0423 \\ 0.0479 \\ 0.0536 \\ 0.0479 \\ 0.0479 \end{bmatrix}$$

$$W_{Privacy\ sub-factors} = \begin{bmatrix} P \\ P_2 \\ P_3 \\ P_4 \\ P_5 \end{bmatrix} = 0.202 \times \begin{bmatrix} 0.14 \\ 0.21 \\ 0.23 \\ 0.18 \\ 0.24 \end{bmatrix} = \begin{bmatrix} 0.0283 \\ 0.0424 \\ 0.0465 \\ 0.0364 \\ 0.0485 \end{bmatrix}$$

$$W_{Legal\ sub-factors} = \begin{bmatrix} L_1 \\ L_2 \\ L_3 \\ L_4 \\ L_5 \end{bmatrix} = 0.176 \times \begin{bmatrix} 0.2 \\ 0.2 \\ 0.2 \\ 0.17 \\ 0.23 \end{bmatrix} = \begin{bmatrix} 0.035 \\ 0.035 \\ 0.035 \\ 0.030 \\ 0.040 \end{bmatrix}$$

$$W_{Business\ sub-factors} = \begin{bmatrix} B_1 \\ B_2 \\ B_3 \\ B_4 \end{bmatrix} = 0.183 \times \begin{bmatrix} 0.23 \\ 0.26 \\ 0.3 \\ 0.21 \end{bmatrix} = \begin{bmatrix} 0.042 \\ 0.048 \\ 0.055 \\ 0.038 \end{bmatrix}$$

$$W_{Cultural\ sub-factors} = \begin{bmatrix} C_1 \\ C_2 \\ C_3 \\ C_4 \end{bmatrix} = 0.157 \times \begin{bmatrix} 0.22 \\ 0.31 \\ 0.22 \\ 0.25 \end{bmatrix} = \begin{bmatrix} 0.034 \\ 0.049 \\ 0.034 \\ 0.039 \end{bmatrix}$$

According to Table 10, the most important factors are “technological”, “privacy and security” and “business”, respectively. By comparing global weights of the factors, it is obvious that “technological” factor is far more important than other factors. On the other hand, the difference in the weight of “privacy and security” and “business” is not substantial. Similarly, the most important sub-factors are “business model”, “architecture and design” and “education and training”, respectively. It can easily be concluded that the first two sub-factors are significantly more important than the rest.

The findings of this study correspond to previous research in most cases. For instance, “Business model” has been identified as the most important challenge in Iran which other researchers such as [30] and [44] also referred to its importance. Besides [29], has mentioned the importance of “architecture and design”, which was ranked 2nd in this study. The sub-factor “education and training” however, has received little attention in other researches to the best of our knowledge (Table 11). More details are provided in Table 2.

There are two studies, however, that reported different

Table 4
Local weight of business challenges.

Business challenges	Economic and development	Investing	Business model	Customer expectations	Calculated weights
Economic and development	(1,1,1)	(1/2,1,3/2)	(1/2,2/3,1)	(2/3,1,2)	0.23
Investing	(2/3,1,2)	(1,1,1)	(1/2,1,3/2)	(2/3,1,2)	0.26
Business model	(1,3/2,2)	(2/3,1,2)	(1,1,1)	(1,3/2,2)	0.30
Customer expectations	(1/2,1,3/2)	(1/2,1,3/2)	(1/2,2/3,1)	(1,1,1)	0.21

Consistency index (λ^*) = 0.78.

Table 5
Local weight of cultural challenges.

Cultural challenges	Trust	Education and training	vandalism	Ethics	Calculated weights
Trust	(1,1,1)	(1/2,2/3,1)	(2/3,1,2)	(2/3,1,2)	0.22
Education and training	(1,3/2,2)	(1,1,1)	(1,3/2,2)	(2/3,1,2)	0.31
Vandalism	(1/2,1,3/2)	(1/2,2/3,1)	(1,1,1)	(2/3,1,2)	0.22
Ethics	(1/2,1,3/2)	(1/2,1,3/2)	(1/2,1,3/2)	(1,1,1)	0.25

Consistency index (λ*) = 0.85.

Table 6
Local weight of legal challenges.

Legal challenges	Ownership	Standardization	Cross boarder	liability	Data usage	Calculated weights
Ownership	(1,1,1)	(2/3,1,2)	(2/3,1,2)	(2/3,1,2)	(1/2,1,3/2)	0.20
Standardization	(1/2,1,3/2)	(1,1,1)	(1/2,1,3/2)	(2/3,1,2)	(1/2,1,3/2)	0.20
Cross boarder	(1/2,1,3/2)	(2/3,1,2)	(1,1,1)	(2/3,1,2)	(1/2,1,3/2)	0.20
liability	(1/2,1,3/2)	(1/2,1,3/2)	(1/2,1,3/2)	(1,1,1)	(1/2,2/3,1)	0.017
Data usage	(2/3,1,2)	(2/3,1,2)	(2/3,1,2)	(1,3/2,2)	(1,1,1)	0.23

Consistency index (λ*) = 0.79.

Table 7
Local weight of technological challenges.

Technological challenges	Hardware	Fault tolerance	Device	Architecture	Ubiquitous	Addressing	Calculated weights
Hardware	(1,1,1)	(2/3,1,2)	(1/2,1,3/2)	(1/2,2/3,1)	(1/2,1,3/2)	(1/2,1,3/2)	0.15
Fault tolerance	(1/2,1,3/2)	(1,1,1)	(1/2,1,3/2)	(1/2,2/3,1)	(1/2,1,3/2)	(1/2,1,3/2)	0.15
Device	(2/3,1,2)	(2/3,1,2)	(1,1,1)	(1/2,1,3/2)	(2/3,1,2)	(2/3,1,2)	0.17
Architecture	(1,3/2,2)	(1,3/2,2)	(2/3,1,2)	(1,1,1)	(2/3,1,2)	(2/3,1,2)	0.19
Ubiquitous	(2/3,1,2)	(2/3,1,2)	(1/2,1,3/2)	(1/2,1,3/2)	(1,1,1)	(2/3,1,2)	0.17
Addressing	(2/3,1,2)	(2/3,1,2)	(1/2,1,3/2)	(1/2,1,3/2)	(1/2,1,3/2)	(1,1,1)	0.17

Consistency index (λ*) = 0.74.

Table 8
Local weight of privacy challenges.

Privacy challenges	conflict	Transparency	Network	IoT device	Data	Calculated weights
conflict	(1,1,1)	(2/3,1,2)	(2/3,1,2)	(1,1,1)	(1/2,2/3,1)	0.14
Transparency	(1/2,1,3/2)	(1,1,1)	(1/2,1,3/2)	(1/2,1,3/2)	(2/3,1,2)	0.21
Network	(1/2,1,3/2)	(2/3,1,2)	(1,1,1)	(1,3/2,2)	(2/3,1,2)	0.23
IoT device	(1,1,1)	(2/3,1,2)	(1/2,2/3,1)	(1,1,1)	(1/2,2/3,1)	0.18
Data	(1,3/2,2)	(1/2,1,3/2)	(1/2,1,3/2)	(1,3/2,2)	(1,1,1)	0.24

Consistency index (λ*) = 0.71.

Table 9
Local weight of factors.

factors	Tech	Privacy	Legal	Business	Cultural	Calculated weights
Tech	(1,1,1)	(1/2,1,3/2)	(1,3/2,2)	(2/3,1,2)	(1,3/2,2)	0.24
Privacy	(2/3,1,2)	(1,1,1)	(2/3,1,2)	(2/3,1,2)	(1,3/2,2)	0.22
Legal	(1/2,2/3,1)	(1/2,1,3/2)	(1,1,1)	(2/3,1,2)	(1,1,1)	0.18
Business	(1/2,1,3/2)	(1/2,1,3/2)	(1/2,1,3/2)	(1,1,1)	(2/3,1,2)	0.20
Cultural	(1/2,2/3,1)	(1/2,2/3,1)	(1,1,1)	(1/2,1,3/2)	(1,1,1)	0.16

Consistency index (λ*) = 0.75.

results. According to [16], which examined the challenges of the business model in IoT, standardization, architecture and design, economic issues and customer expectations were ranked as the most important challenges, while in this study the aforementioned challenges ranked 18th, 2nd, 13th and 16th. Furthermore [18], which considered the vital security requirements of IoT, selected trust, fault tolerance, network security, addressing and data confidentiality as the most substantial challenges, while in this study the aforementioned challenges ranked 21st, 11th, 9th, 6th and 4th.

5. Conclusion

In recent years, the Internet of Things has been of prime interest to policy-makers and business owners as an emerging technology. Iran, as a transition economy from factor-driven to efficiency-driven economy, has shown increasing interest in IoT and has carried out some efforts in ITRC.

This article categorized the Internet of Things technology development challenges in Iran into five categories, namely security and privacy challenges, legal and regulatory challenges, technological challenges, cultural challenges and business challenges

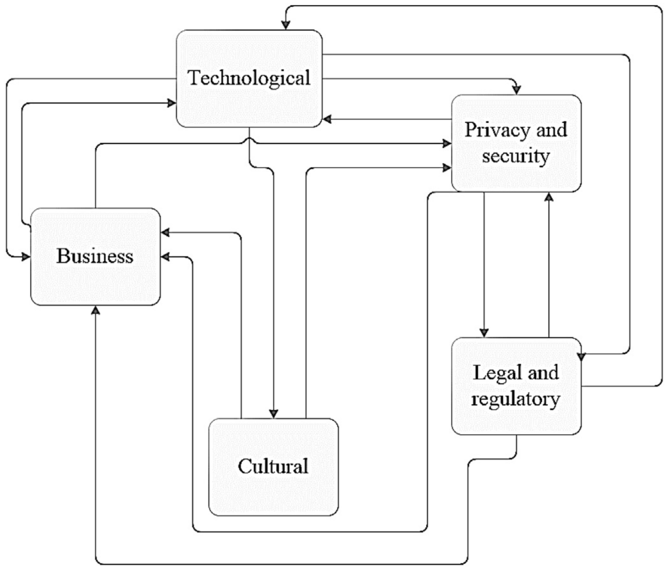

Fig. 2. Relationships between factors.

Table 10
Interdependent weights of the factors.

factors	Tech	Privacy	Legal	Business	Cultural
Tech	0.75	0.1	0.15	0.15	0.15
Privacy	0.1	0.65	0.2	0.05	0
Legal	0.15	0.15	0.65	0.05	0
Business	0	0.05	0	0.70	0
Cultural	0	0.05	0	0.05	0.85

which include 24 sub-factors. In the second phase, the importance and priority of these factors and sub-factors were identified using an integrated fuzzy ANP approach. According to experimental results, “technological challenges” and “privacy and security challenges” were ranked the two most important factors. Besides, the factors “cultural challenges” was ranked as the least significant factor.

Among the sub-factors, however, the most important sub-factor which affects IoT technology development is “business model”. The sub-factors “architecture and design” and “education and training” are ranked 2nd and 3rd respectively. On the other hand, “conflict of interests” and “liability” were selected as the least important ones.

Considering the results of this study, a series of suggestions are presented for future studies and practices. Considering the great importance of business models, it is suggested that new business models be analyzed by utilizing state of the art strategic frameworks. Saleability and reliability are at the heart of designing and implementing such business models. It is also essential not to neglect the basic dimensions, such as customers and ecosystem, in IoT business models.

Hitherto, some developed countries have implemented huge projects in IoT and the majority of such investments have been made by the governments. In order to provide infrastructure for implementing IoT in Iran, it is suggested that the public sector be more active. Moreover, in order to overcome the technological challenge in the implementation of IoT in Iran, it is suggested that the key essential technologies for the success of IoT based products and services (such as RFID, WSN and cloud computing) be investigated and the development of infrastructures related to such technologies be put on the agenda.

Finally, considering the importance of “privacy and security”, it is necessary to limit the collection of private data such as health, religion and sexual orientation when they are not absolutely essential. Besides, in case obtaining such data is absolutely necessary, such as healthcare applications, data collected by IoT devices should not be stored, processed or revealed in any form without the individual's consent. Hence, clear regulatory framework must be provided as well as technical measures which ensure the privacy of the collected data.

In this study the challenges were identified before any major implementation in industry. That is because as the responsible institution for providing the IoT roadmap in Iran, ITRC should have

Table 11
Global weight and rank for factors and sub-factors.

Factors	Sub-factors	Global weight	Rank
Technological	Architecture and design	0.0536	2
(0.282)	Devices heterogeneity	0.0479	6
	Addressing	0.0479	6
	Ubiquitous data management	0.0479	6
	Hardware construction	0.0423	11
	Fault tolerance	0.0423	11
Privacy & Security	Data confidentiality	0.0485	4
(0.202)	Network security	0.0465	9
	Transparency	0.0424	10
	IoT devices' safety	0.0364	17
	Conflict of interests	0.0283	24
Business	Business model	0.0550	1
(0.183)	Investing in IoT development	0.0480	5
	Economic and development opportunities and issues	0.0420	13
	Customer expectations and Quality of service	0.0380	16
Legal & regulatory	Data usage	0.0400	14
(0.176)	Ownership	0.0350	18
	Standardization	0.0350	18
	Cross boarder data flows and Global cooperation	0.0350	18
	Liability	0.0300	23
Cultural	Education and training	0.0490	3
(0.157)	Ethics	0.0390	15
	Trust	0.0340	21
	Vandalism	0.0340	21

an understanding of the challenges ahead prior to any further action. Due to this matter, major actors in industrial sector did not have a clear understanding of the challenges ahead. Hence, only the views of academic experts and policy makers were applied in this study which has been the main constraint facing this research.

This study aimed at identifying and prioritizing the IoT technology development challenges in Iran. However, the interactions amongst the factors may be different in other cases. Such relations can be inspected within the scope of future studies. Furthermore, due to the importance of technological challenges regarding IoT technology development, a study can be made to exclusively analyze the aforementioned challenge.

Acknowledgement

This research has been supported by the department of business and entrepreneurship of the Iran Telecommunication Research Center (ITRC), under the grant number 9334113.

Appendix A. Supplementary data

Supplementary data related to this article can be found at https://doi.org/10.1016/j.techsoc.2018.01.007.

References

[1] Z.J. Acs, S. Desai, J. Hessels, Entrepreneurship, economic development and institutions, Small Bus. Econ. 31 (3) (Oct. 2008) 219–234.
[2] M. Herrington, P. Kew, Global Entrepreneurship Monitor 2016/2017, 2016.
[3] K. Schwab, World Economic Forum's Global Competitiveness Report, 2014-2015, Retrived from, 2015.
[4] M. Zarei, A. Mohammadian, R. Ghasemi, Internet of things in industries: a survey for sustainable development, Int. J. Innov. Sustain. Dev. 10 (4) (2016) 419–442.
[5] I. Lee, K. Lee, The internet of things (IoT): applications, investments, and challenges for enterprises, Bus. Horiz. 58 (4) (2015) 431–440.
[6] L. Da Xu, W. He, S. Li, Internet of things in industries: a survey, IEEE Trans. Ind. informatics 10 (4) (2014) 2233–2243.
[7] D. Lund, C. MacGillivray, V. Turner, M. Morales, Worldwide and regional internet of things (iot) 2014–2020 forecast: a virtuous circle of proven value and demand, in: Int. Data Corp. (IDC), Tech. Rep, 2014.
[8] L. Coetzee, J. Eksteen, The Internet of Things-promise for the future? An introduction, in: IST-Africa Conference Proceedings, vol. 2011, 2011, pp. 1–9.
[9] L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Comput. Network. 54 (15) (Oct. 2010) 2787–2805.
[10] D. Giusto, A. Iera, G. Morabito, L. Atzori, The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications, Springer Science & Business Media, 2010.
[11] M. Zarei, A. Jamalian, R. Ghasemi, Industrial guidelines for stimulating entrepreneurship with the internet of things, in: The Internet of Things in the Modern Business Environment, IGI Global, 2017, pp. 147–166.
[12] T. Xu, J.B. Wendt, M. Potkonjak, Security of IoT systems: design challenges and opportunities, in: Proceedings of the 2014 IEEE/ACM International Conference on Computer-aided Design, 2014, pp. 417–423.
[13] N. Heo, Deployment issues for the internet of things: a survey, Int. Inf. Inst. (Tokyo). Inf. 18 (4) (2015) 1313.
[14] R.H. Weber, Internet of Things–New security and privacy challenges, Comput. Law Secur. Rep. 26 (1) (2010) 23–30.
[15] K. Al-mabrouk, J. Soar, An analysis of the major issues for successful information technology transfer in Arab countries, Int. Arab J. Inf. Technol. 6 (1) (2009) 7–15.
[16] N. Azad, K. Dehbasteh, IOT based framework for Telco Business Model using Fuzzy method, Int. J. Hum. Comput. Stud. (2016) 455–470. ISSN 2356-5926.
[17] R. Mousa, E-government challenges at the UK's customs and tax department, Electron. Gov. an Int. J. 10 (1) (2013) 86.
[18] K.C. Park, D.-H. Shin, Security assessment framework for IoT service, Telecommun. Syst. 64 (1) (2017) 193–209.
[19] I. Syamsuddin, J. Hwang, A new fuzzy MCDM framework to evaluate e-government security strategy, in: Application of Information and Communication Technologies (AICT), 2010 4th International Conference on, 2010, pp. 1–5.
[20] G. Harman, M. Hayden, P.T. Nghi, Higher education in Vietnam: reform, challenges and priorities, in: Reforming Higher Education in Vietnam, Springer, 2010, pp. 1–13.
[21] S.R. Moosavi, T.N. Gia, E. Nigussie, A.M. Rahmani, S. Virtanen, H. Tenhunen, J. Isoaho, End-to-end security scheme for mobility enabled healthcare Internet of Things, Future Generat. Comput. Syst. 64 (2016) 108–124.
[22] B.D. Weinberg, G.R. Milne, Y.G. Andonova, F.M. Hajjat, Internet of Things: convenience vs. privacy and secrecy, Bus. Horiz. 58 (6) (2015) 615–624.
[23] C. Tankard, The security issues of the Internet of Things, Comput. Fraud Secur. 2015 (9) (2015) 11–14.
[24] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Network. 57 (10) (2013) 2266–2279.
[25] K. Rose, S. Eldridge, L. Chapin, The internet of things: an overview, Internet Soc. (2015) 1–50.
[26] R.H. Weber, Internet of things: privacy issues revisited, Comput. Law Secur. Rev. 31 (5) (2015) 618–627.
[27] D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac, Internet of things: vision, applications and research challenges, Ad Hoc Netw. 10 (7) (Sep. 2012) 1497–1516.
[28] G. Padmavathi, IOT security challenges and issues-an overview, World Sci. News 41 (2016) 232.
[29] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions, Future Generat. Comput. Syst. 29 (7) (Sep. 2013) 1645–1660.
[30] S. Chen, H. Xu, D. Liu, B. Hu, H. Wang, A vision of IoT: applications, challenges, and opportunities with China perspective, IEEE Internet Things J. 1 (4) (2014) 349–359.
[31] C. Alcaraz, P. Najera, J. Lopez, R. Roman, Wireless sensor networks and the internet of things: do we need a complete integration?, in: 1st International Workshop on the Security of the Internet of Things (SecIoT'10), 2010.
[32] A. Botta, W. De Donato, V. Persico, A. Pescapé, Integration of cloud computing and internet of things: a survey, Future Generat. Comput. Syst. 56 (2016) 684–700.
[33] E. Borgia, The Internet of Things vision: key features, applications and open issues, Comput. Commun. 54 (2014) 1–31.
[34] D. Bandyopadhyay, J. Sen, Internet of things: applications and challenges in technology and standardization, Wireless Pers. Commun. 58 (1) (2011) 49–69.
[35] I. Gartner, Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations that Organizations Should Monitor, August, 2015.
[36] J. Yang, B. Fang, Security model and key technologies for the Internet of things, J. China Univ. Posts Telecommun. 18 (2011) 109–112.
[37] A. Adshead, Data set to grow 10-fold by 2020 as internet of things takes off, Comput. com 9 (2014).
[38] J. Manyika, M. Chui, B. Brown, J. Bughin, R. Dobbs, C. Roxburgh, A.H. Byers, Big Data: the Next Frontier for Innovation, Competition, and Productivity, 2011. http//www. mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_ for_innovation. vol. 5, no. 33, p. 222, 2014.
[39] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, Vision and challenges for realising the internet of things, Clust. Eur. Res. Proj. Internet Things, Eur. Commision (3) (2010) 34–36.
[40] L. Sanchez, L. Muñoz, J.A. Galache, P. Sotres, J.R. Santana, V. Gutierrez, R. Ramdhany, A. Gluhak, S. Krco, E. Theodoridis, SmartSantander: IoT experimentation over a smart city testbed, Comput. Network. 61 (2014) 217–238.
[41] Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for Internet of Things, J. Netw. Comput. Appl. 42 (2014) 120–134.
[42] R. Van Kranenburg, A. Bassi, IoT challenges, Commun. Mob. Comput. 1 (1) (2012) 9.
[43] R.M. Dijkman, B. Sprenkels, T. Peeters, A. Janssen, Business models for the internet of things, Int. J. Inf. Manag. 35 (6) (2015) 672–678.
[44] T. Zachariah, N. Klugman, B. Campbell, J. Adkins, N. Jackson, P. Dutta, The internet of things has a gateway problem, in: Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications, 2015, pp. 27–32.
[45] L. Gronholdt, A. Martensen, K. Kristensen, The relationship between customer satisfaction and loyalty: cross-industry differences, Total Qual. Manag. 11 (4–6) (2000) 509–514.
[46] R. Hallowell, The relationships of customer satisfaction, customer loyalty, and profitability: an empirical study, Int. J. Serv. Ind. Manag. 7 (4) (1996) 27–42.
[47] Y.U. Jie, N. Subramanian, K. Ning, D. Edwards, Product delivery service provider selection and customer satisfaction in the era of internet of things: a Chinese e-retailers' perspective, Int. J. Prod. Econ. 159 (2015) 104–116.
[48] D.-H. Shin, Conceptualizing and measuring quality of experience of the internet of things: exploring how quality is perceived by users, Inf. Manag. (8) (2017) 998–1011.
[49] C. Lin, C.N. Madu, C. Kuei, H.-L. Tsai, K. Wang, Developing an assessment framework for managing sustainability programs: a Analytic Network Process approach, Expert Syst. Appl. 42 (5) (2015) 2488–2501.
[50] T.L. Saaty, Fundamentals of the Analytic Network Process, University of Pittsburgh, Pittsburgh, USA, 1999.
[51] M. Dağdeviren, İ. Yüksel, A fuzzy analytic network process (ANP) model for measurement of the sectoral competititon level (SCL), Expert Syst. Appl. 37 (2) (2010) 1005–1014.
[52] Z. Ayağ, R.G. Özdemir, Evaluating machine tool alternatives through modified TOPSIS and alpha-cut based fuzzy ANP, Int. J. Prod. Econ. 140 (2) (2012) 630–636.
[53] N.S. Arunraj, S. Mandal, J. Maiti, Modeling uncertainty in risk assessment: an integrated approach with fuzzy set theory and Monte Carlo simulation, Accid. Anal. Prev. 55 (2013) 242–255.
[54] L.A. Zadeh, Fuzzy Sets, Fuzzy Logic, and Fuzzy Systems: Selected Papers by

Please cite this article in press as: A.K. Mohammadzadeh, et al., A Fuzzy Analytic Network Process (FANP) approach for prioritizing internet of things challenges in Iran, Technology in Society (2018), https://doi.org/10.1016/j.techsoc.2018.01.007

Lotfi a Zadeh, vol. 6, World Scientific, 1996.

[55] K. Hirota, M. Sugeno, Industrial Applications of Fuzzy Technology in the World, vol. 2, World Scientific, 1995.

[56] P.P. Wang, Advances in Fuzzy Sets, Possibility Theory, and Applications, Springer Science & Business Media, 2012.

[57] M.A.B. Promentilla, T. Furuichi, K. Ishii, N. Tanikawa, A fuzzy analytic network process for multi-criteria evaluation of contaminated site remedial countermeasures, J. Environ. Manag. 88 (3) (2008) 479–495.

[58] A. Dargi, A. Anjomshoae, M.R. Galankashi, A. Memari, M.B.M. Tap, Supplier selection: a fuzzy-ANP approach, Procedia Comput. Sci. 31 (2014) 691–700.

[59] B. Oztaysi, T. Gurbuz, E. Albayrak, C. Kahraman, Target marketing strategy determination for shopping malls using fuzzy ANP, J. Mult. Log. Soft Comput. 27 (2016).

[60] A.Ç. Tolga, F. Tuysuz, C. Kahraman, Fuzzy real option value integrated fuzzy ANP method for location selection problems, in: Fuzzy Systems (FUZZ), 2010 IEEE International Conference on, 2010, pp. 1–9.

[61] O. Senvar, U.R. Tuzkaya, C. Kahraman, Supply chain performance measurement: an integrated DEMATEL and fuzzy-ANP approach, in: Supply Chain Management under Fuzziness, Springer, 2014, pp. 143–165.

[62] L. Mikhailov, P. Tsvetinov, Evaluation of services using a fuzzy analytic hierarchy process, Appl. Soft Comput. 5 (1) (2004) 23–33.

[63] B.D. Rouyendegh, T.E. Erkan, An application of the fuzzy electre method for academic staff selection, Hum. Factors Ergon. Manuf. Serv. Ind. 23 (2) (2013) 107–115.

[64] I. Etikan, R. Alkassim, S. Abubakar, Comparision of snowball sampling and sequential sampling technique, Biometrics Biostat. Int. J. 3 (1) (2016) 55.

[65] D.D. Heckathorn, Comment: snowball versus respondent-driven sampling, Socio. Meth. 41 (1) (2011) 355–366.

[66] T.L. Saaty, Homogeneity and clustering in AHP ensures the validity of the scale, Eur. J. Oper. Res. 72 (3) (1994) 598–601.

[67] C. Kahraman, T. Ertay, G. Büyüközkan, A fuzzy optimization model for QFD planning process using analytic network approach, Eur. J. Oper. Res. 171 (2) (2006) 390–411.

Mr. Ali Kamali Mohammadzadeh. Ali Kamali Mohammadzadeh was born in Bandar Anzali, Iran, 1983. He graduated from the University of Tehran, Tehran, Iran, in Industrial Management, in 2012, and received his M.Sc. degree from the University of Tehran, Tehran, Iran, in Operation Research, in 2015. His general research interests include time series analysis, big data analytics and optimization.

Mr. Saeed Ghafoori. Saeed Ghafoori completed his MSc in Operation Research at the University of Tehran, Tehran, Iran in 2015. Project management, decision making and optimization are among his research interests.

Dr. Ayoub Mohammadian. Dr. Ayoub Mohammadian is Assistant professor of information technology (IT) management at University of Tehran. He earned his B.S. in Business Administration and his M.A. and Ph.D. in IT management from University of Tehran. In addition to teaching, He is founder and director of Digital Business Innovation (DBI) research group at the faculty of management. He was honored with the Award for his contributions to national e-government project in Iran's ministry of commerce. He is author of more than 40 scholarly articles in academic journals and conferences. His recent research focuses on the internet of things business value and challenges.

Dr. Reza MohammadKazemi. Reza MohammadKazemi is an Associated Professor in Faculty of Entrepreneurship at University of Tehran and he is head of new business department in this faculty. His Ph.D. in Sport Management & marketing through sport. He started to teach marketing and entrepreneurship in Faculty of entrepreneurship in 2008. More than 30 of his papers on marketing & service businesses. Exporting of service business's facilities is also in his interested area in which he supervised Student's Master Thesis. Moreover to teaching Business and marketing, he has much experience in international service business in the Middle East Zone.

Ms. Bahareh Mahbanooei. Bahareh Mahbanooei is an Organizational Behavior Management PhD Candidate at University of Tehran, Tehran, Iran. She earned her B.S. in Public Administration and her M.A. in Human Resource Management from University of Tehran as well. She was a Tax Expert in National Tax Admission Organization of Iran. In addition, she teaches the Industrial relations and Industrial safety at university of Tehran. She has written several papers on eHealth ethics in hospitals, global competitiveness, competency management and empowerment. Her recent research interest focuses on eHealth ethics, Business ethics, and managerial competencies.

Dr. Rohollah Ghasemi. Rohollah Ghasemi is a visiting Lecturer in the Faculty of Management, University of Tehran. He completed his PhD in Production and Operations Management at the University of Tehran, following several years of working experience in industry (especially: Iran Telecommunication Research Center (ITRC)). His focal area of research was the subject of Internet of things that led to a number of high quality publications. His research has been extended to other areas including Supply chain Management, Strategic Management, Business Process Improvement and Quality Management. Rohollah's research has involved engaging with organizations and industry at various capacities. He has supervised several M.Sc. students successfully.

Please cite this article in press as: A.K. Mohammadzadeh, et al., A Fuzzy Analytic Network Process (FANP) approach for prioritizing internet of things challenges in Iran, Technology in Society (2018), https://doi.org/10.1016/j.techsoc.2018.01.007