Telecommun Syst (2017) 64:193–209
DOI 10.1007/s11235-016-0168-0

Security assessment framework for IoT service

Keon Chul Park[1] · **Dong-Hee Shin**[1]

Published online: 13 May 2016

Abstract What are the critical requirements to be considered for the security measures in Internet of Things (IoT) services? Further, how should those security resources be allocated? To provide valuable insight into these questions, this paper introduces a security assessment framework for the IoT service environment from an architectural perspective. Our proposed framework integrates fuzzy DEMATEL and fuzzy ANP to reflect dependence and feedback interrelations among security criteria and, ultimately, to weigh and prioritize them. The results, gleaned from the judgments of 38 security experts, revealed that security design should put more importance on the service layer, especially to ensure availability and trust. We believe that these results will contribute to the provision of more secure and reliable IoT services.

Keywords Internet of Things · Security requirement · Security assessment · Fuzzy set theory

The information age, created by the rapid advancement of information and communications technology (ICT) and the widespread adoption of wireless technologies, has presented an exciting new capability for both humans and diverse applications to extend the interconnectivity through the new dimension of "things" communication and integration [21]. Cisco predicts that by 2020, 50 billion things will be connected to the Internet via Internet of Things (IoT) technologies, generating revenues in excess of $19 trillion for industries worldwide [32].

✉ Dong-Hee Shin
dshin@skku.edu

[1] Department of Interaction Science, Sungkyunkwan University, Myeongnyun-dong, Jongno-gu, Seoul 110-745, South Korea

As defined by Shin [42], IoT is a global network infrastructure, linking physical and virtual objects through the exploitation of data and communication capabilities that involves a high degree of autonomous data capture, event transfer, network connectivity, and interoperability. IoT is becoming increasingly omnipresent at the service level, allowing people and things to be connected anytime, anyplace, with anything and anyone, ideally using Any path/network and Any service [21]. As IoT proliferates throughout hyper-connected society, significant opportunities in a variety of industries and services, including healthcare, home network (e.g., smart home), urban planning, energy (e.g., smart grid), and agriculture, will be created using this new technology. Indeed, its powerful and potentially disruptive impact will be felt across all industries and all areas of society [28].

Combined with preeminent technologies such as big data, social media, and cloud, the interconnected "things" (e.g., sensors and smart mobile) monitor and collect nearly all kinds of data from any event or process in order to provide advanced and intelligent services for hyper-connected society [57]. However, as with many new technologies, there are several challenges when it comes to achieving success in IoT adoption. Two of the biggest concerns for manufacturers, developers, service providers, and end-users are security and privacy [38,55].

From a technical perspective, increased accessibility and a simplified procedure for accessing the network means an environment that is rather susceptible to security threats, such as spoofing, tampering, repudiation, information disclosure, denial of service (DoS), and elevation of privilege, which undermine data confidentiality and user privacy [35,54]. In fact, the ubiquitousness of wireless channels and media for exchanging data in real-time increases the risk of violation from remote access capabilities, which potentially

expose the system to eavesdropping and masking attacks [31].

Because IoT not only deals with huge amounts of sensitive data but also has the power to influence both the physical and virtual environment with its control abilities, securing the network and system and protecting user privacy must be considered as the top priority [1]. Although security research has been extensively addressed within the information systems (IS) discipline, there is a great need for a deeper understanding of how to achieve security in the IoT environment. Moreover, although strategic decisions regarding security depend on the fundamental question of how to allocate security resources within the key security requirements and their elements [45], a limited number of studies discuss specifically how to evaluate and make decisions regarding IoT security strategy. Therefore, the main purpose of this research is to investigate key security requirements in IoT architecture and to introduce a security assessment framework for IoT service.

Assessing the various aspects and requirements of IS (e.g., IoT) security is a complex process, as it involves both objective and subjective conditions of information, qualitative assessments on the effect, and the consideration of multiple and conflicting criteria. This multidimensional nature of IoT security assessment justifies the use of multicriteria decision-making (MCDM) methods in which the criteria being considered can be both qualitative and quantitative and usually involve different units of measurement [47,49].

In this study, an integrated fuzzy MCDM (FMCDM) approach has been applied to propose a general security assessment framework for IoT service. The integrated method uses an analytic network process (ANP) in combination with the decision-making trial and evaluation laboratory (DEMATEL) technique under fuzzy set theory in order to increase the sensitivity of interrelationships among diverse security requirements.

First, the fuzzy DEMATEL is applied to derive cause-and-effect interrelationships between the criteria of IoT security requirements. Then, based on the information gained from the fuzzy DEMATEL, fuzzy ANP is implemented to calculate the weight of each security requirement and, finally, to introduce the security assessment framework for IoT service. The main contribution of this research lies in the fact that it will provide practitioners and researchers with implications on how to design security-related IoT services.

The remainder of this paper is organized as follows: Sect. 2 provides a review of the literature regarding the basic concept of IoT and its architectures. A hybrid FMCDM model integrating DEMATEL and ANP with fuzzy set theory is introduced in Sect. 3. An empirical analysis is illustrated in Sect. 4. The last section presents conclusions.

1 Security requirements for IoT service

In this section, to derive the security criteria to be considered in the overall security assessment framework for the IoT service environment, we review key concepts about the security mechanisms and requirements used to address security considerations in IoT architecture.

Security and privacy are critical to the safe and reliable operation of IoT service. The number of things connected to the network for IoT service is increasing rapidly, which raises a significant security risk to users and service providers. IoT presents a variety of potential security risks that can be exploited to harm both the system operation and user device by (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating risks to personal safety. Perceived risks to privacy and security in users, even if not realized, would seriously undermine confidence in the ability of these technologies to meet their full potential, and may constrain the widespread adoption of the technology itself [17]. Thus, in order for IoT services to be beneficial to industry and end-users, data and service security is a basic requirement.

If system-level security (e.g., confidentiality, integrity, authenticity, and privacy of user data) is not ensured, IoT applications will not be adopted on a large scale by the relevant stakeholders [31]. One of the main security challenges comes from a distinct feature of IoT: (device) heterogeneity. IoT aims to interconnect a vast amount of heterogeneous devices (e.g., sensors, RFID, and smart mobile) to provide advanced applications in various fields. This high level of heterogeneity provides a great potential to influence the network and protocol security [31,38]. Furthermore, as identified by Europol [15] in 2014: “With more objects being connected to the Internet and the creation of new types of critical infrastructure, we can expect to see (more) targeted attacks on existing and emerging infrastructures, including new forms of blackmailing and extortion schemes (e.g., ransomware for smart cars or smart homes), data theft, physical injury and possible death, and new types of botnets.” In other words, the more chances there are to access the network, the more vulnerabilities there are to exploit [15,26].

The inherent complexity of IoT, where thousands of entities scattered throughout various contexts and applications, further complicates the design of scalable security mechanisms [38]. IoT needs to be built in a way that ensures easy and safe user control. For users to fully embrace the application and enjoy its potential benefits, they must be confident that it poses no major risks to their security and privacy [19].

Although the literature on security-related topics related to the IoT environment is still in its infancy, there is a substantial body of work that investigates the security considerations that are critical fulfilling the security requirement in IoT applications [2,4,12,22,33,37]. Most of research has agreed that

Table 1 Conventional security requirements for the IoT environment

Requirement	Description	Literature					
		[2]	[37]	[12]	[4]	[33]	[22]
Confidentiality	Transmitted data can be read only by the communication endpoints	o	o	o	o	o	o
Integrity	Received data are not tampered with during transmission; if this does not happen, then any change can be detected	o	o	o	o	o	o
Availability	The communication endpoints can always be reached and cannot be made inaccessible	o	o	o	o	o	o
Authentication	Data sender can always be verified, and data receivers cannot be spoofed	o	o	o	o	o	o
Authorization	Anonymous interaction shall be enabled, as well as group authorization	o				o	o
Access control	Information providers must be able to implement access control on the data provided	o			o		o
Trust	Trust is needed in the interaction between entities. Specifically, the user must trust the system	o					o
Auditing	Users' interactions with the system should be tracked, such as when they access services, who is making the service request, and when the request is happening	o					
Reputation metering	As there is a high chance of nodes being compromised due to their physical availability to malicious users, a secondary mechanism for establishing trust is needed						o
Privacy	Measures need to be taken that only the information provider is able to infer from observing the use of the lookup system related to a specific customer; at a minimum, inference should be very hard to conduct	o			o	o	
Anonymization	If proper countermeasures are not taken, even users employing pseudonyms could be tracked by their network locator						o
Accountability	Some services could be classified or critical for their provider and could require users to take responsibility for their action. On the other hand, users might need providers to take responsibility for the services they provide, as relying on such services is critical for them						o
Replay protection	Intermediate node can store a data packet and replay it at a later stage. Thus, mechanisms are needed to detect duplicate or replayed messages		o				
Resilience to attacks	The system has to avoid single points of failure and should adjust itself to node failures			o			
Fault tolerance	Overall service can be delivered even when a number of atomic services are faulty						o
Non-repudiation	Services should be accessible to users who have the right to access them				o	o	o

all common aspects of information security requirements (e.g., CIA triad) must be considered from the initial stage of IoT system design and development. The conventional security requirements for the IoT environment are described in Table 1.

For this study, we have carefully reviewed the above-mentioned features and functions as well as many other security requirements and solutions. Of course, all of these security requirements are critical for reliable and safe service operations. However, due to the constraints of devices, network congestion, system interoperability and so forth, strategic approaches to designing and allocating these security resources are necessary [43]. Whereas desktop PCs benefit from many add-on security features that increase safety; IoT applications usually use tiny little sensors or mobile devices that have low computing capacity and battery constraints. For this reason, it is necessary to make choices among the security requirements and decide how to allocate those security resources. For these strategic decisions, we first group the security requirements into four logical security components (criteria) based on their functionalities and service architecture. Figure 1 illustrates the security criteria and their sub-criteria to be considered in the IoT service environment.

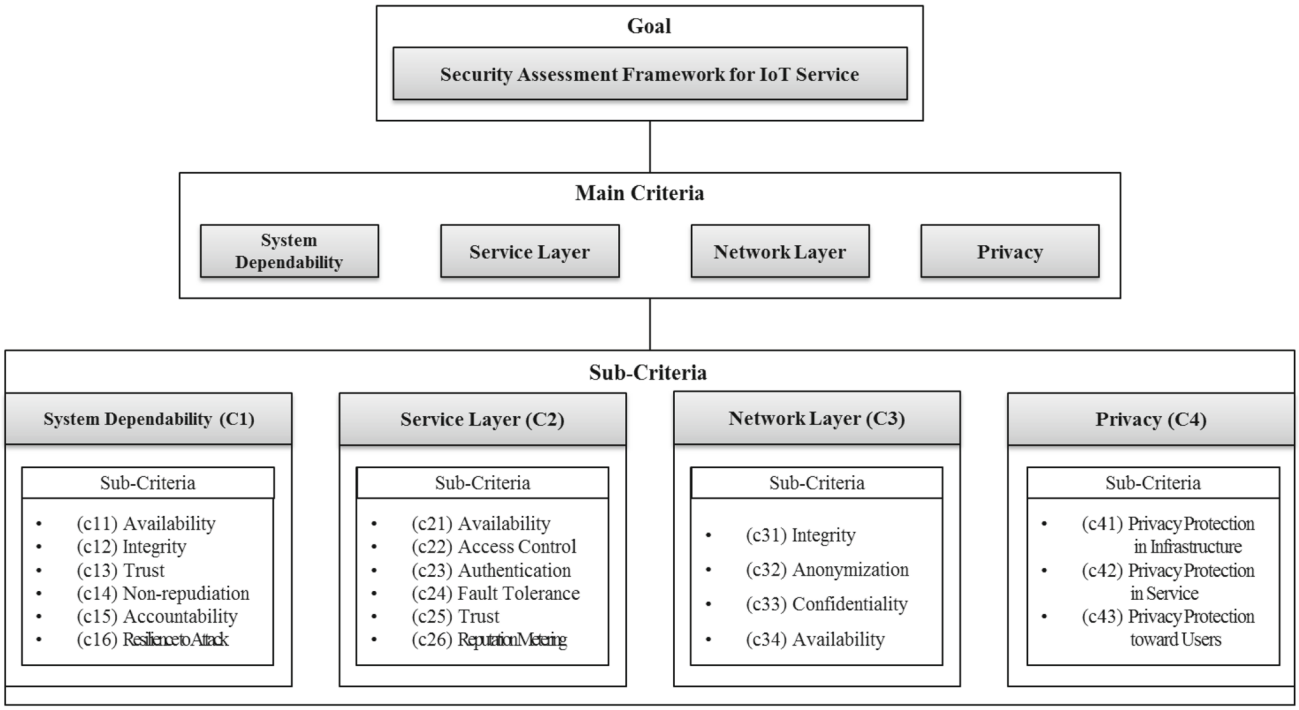


Fig. 1 Security criteria to be considered in IoT service

2 A hybrid MCDM approach to a security assessment framework for IoT service

This study proposes a security assessment framework for IoT service based on a hybrid MCDM model that integrates fuzzy DEMATEL and fuzzy ANP. The general overview of the proposed model and analysis flow is shown in Fig. 2.

2.1 Fuzzy set theory and fuzzy numbers

Fuzzy set theory, introduced by Zadeh [62], is a mathematical method used to explain uncertainty in events or systems where uncertainty arises due to imprecision in the decision process [5]. The imprecision may be from unquantifiable or immeasurable information, inaccessible or incomplete data, or partial ignorance. In many processes of evaluation, judgement, and decision making, natural human languages and linguistic variables are employed to articulate subjective perceptions, and the linguistic terms used might not have a clear and well-defined meaning [46]. When such a linguistic term is applied as a label, the boundaries of the set to which objects do or do not belong will become fuzzy. To better cope with this problem and make more precise judgement, fuzzy logics and fuzzy numbers are applied in order to help linguistic variables be expressed appropriately [27]. When applying fuzzy logic, a linguistic variable can be represented by a fuzzy number assigned to a membership function [47].

Since its initial introduction, fuzzy set theory has proved to be very useful for modelling the kind of uncertainty associated with vagueness in various research fields [27]. Fuzzy logic is useful for modeling linguistic evaluations as it allows for capturing imprecisions, which are interpreted as a form of vagueness [46]. Many uncertain influencers and factors affect security problems. Moreover, in many cases of decisions regarding security strategy, judgements on determining the risk value, risk probability of occurrence of security attack, or the consequence of occurrence of security threat are conducted according to the decision maker's experiences. This implies that substantial level of subjectivity is involved; accordingly, it would be very appropriate to apply the fuzzy concept in this problem [59].

Among fuzzy numbers, triangular fuzzy numbers (TFN) have been identified as useful in quantifying the uncertainty in decision making because of their intuitive appeal, efficiency, and simplicity in computation [20,23].

A TFN is shown in Fig. 3. The TFN is denoted simply as (l, m, u). The parameters l, m, and u, respectively, denote the smallest possible value, the most promising value, and the largest possible value that describe a fuzzy event. Each TFN has linear representations on its left and right side such that its membership function can be defined as follows:

$$\mu_A(x) = \begin{cases} (x-l)/(m-l) & l \le x \le m \\ (u-x)/(u-m) & m \le x \le u \\ 0 & otherwise \end{cases} \quad (1)$$

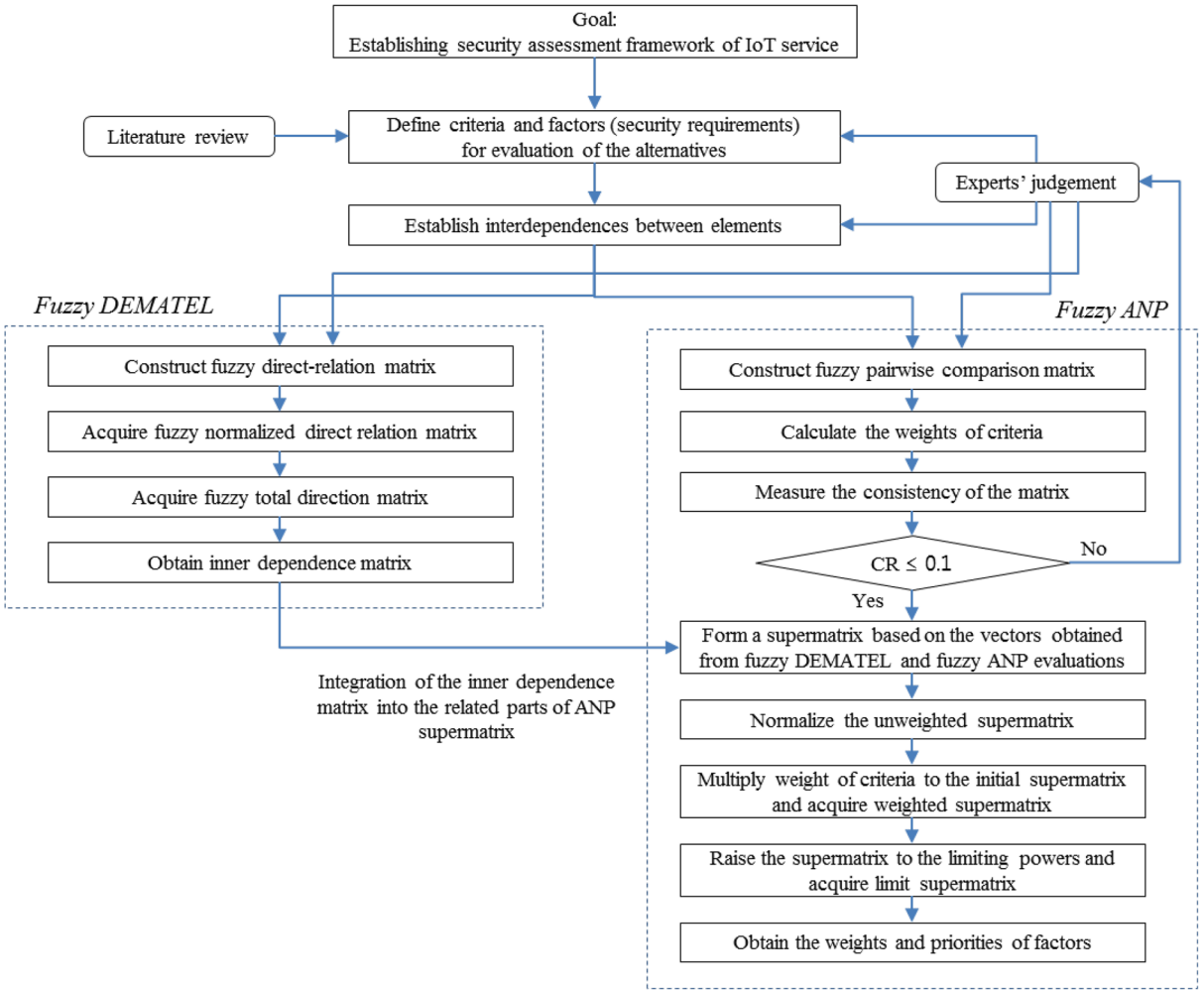


Fig. 2 A proposed hybrid MCDM model and research flow

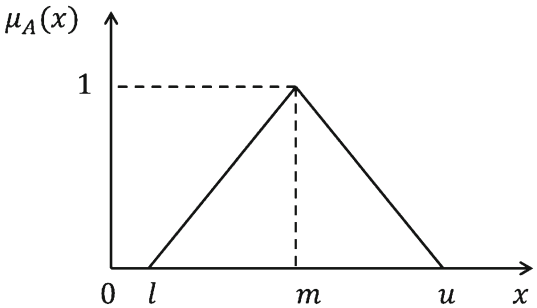


Fig. 3 Triangular fuzzy number

The operational principles for TFNs of two fuzzy numbers $\tilde{A}_1 = (l_1, m_1, u_1)$ and $\tilde{A}_2 = (l_2, m_2, u_2)$ are shown in Eq. (2) [44,46]:

$$\begin{aligned}
\tilde{A}_1\tilde{A}_2 &= (l_1, m_1, u_1) \otimes (l_2, m_2, u_2) \\
&= (l_1 + l_2, m_1 + m_2, u_1 + u_2) \\
\tilde{A}_1\tilde{A}_2 &= (l_1, m_1, u_1) \otimes (l_2, m_2, u_2) = (l_1 l_2, m_1 m_2, u_1 u_2) \\
& \quad l_1 l_2 > 0, m_1 m_2 > 0, u_1 u_2 > 0 \\
\tilde{A}_1 - \tilde{A}_2 &= (l_1, m_1, u_1) - (l_2, m_2, u_2) \\
&= (l_1 - l_2, m_1 - m_2, u_1 - u_2) \\
\tilde{A}_1 \div \tilde{A}_2 &= (l_1, m_1, u_1) \div (l_2, m_2, u_2) = \left(\frac{l_1}{l_2}, \frac{m_1}{m_2}, \frac{u_1}{u_2}\right) \\
& \quad l_1 l_2 > 0, m_1 m_2 > 0, u_1 u_2 > 0
\end{aligned} \tag{2}$$

In our approach, the linguistic variables referring to the importance of the criteria and the ratings of the alternatives are made based on a 5-point scale, as shown in Fig. 4 and Table 2.

2.2 Fuzzy DEMATEL

DEMATEL, which originated from the Geneva Research Centre of the Battelle Memorial Institute, is a comprehensive technique for building and analyzing a structural model involving cause and effect interrelationships between complex criteria [18,52]. DEMATEL helps to analyze the

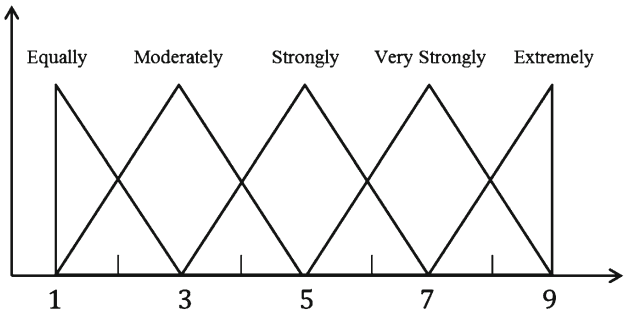


Fig. 4 A fuzzy membership function for linguistic variables

Table 2 Fuzzy linguistic variables

Fuzzy number	Linguistic variable	TFN
$\tilde{1}$	Equally important/preferred	(1, 1, 3)
$\tilde{3}$	Moderately important/preferred	(1, 3, 5)
$\tilde{5}$	Strongly important/preferred	(3, 5, 7)
$\tilde{7}$	Very strongly important/preferred	(5, 7, 9)
$\tilde{9}$	Extremely important/preferred	(7, 9, 9)

influential status and strength between the factors and criteria, and converts them into an explicit structural mode of a system. DEMATEL has been utilized in numerous contexts as a practical tool [7,25,48,56,59,60].

DEMATEL has been proven as a useful method to solve complicated MCDM problems. However, in many MCDM cases, human judgments and preferences are difficult to express in crisp values due to the fuzziness [56,60]. Thus, to address this problem, we applied fuzzy theory to the DEMATEL in order to quantify the qualitative judgments on the interrelationships among security criteria.

The equations and calculation procedures for applying fuzzy DEMATEL are described below [7,10,46]:

2.2.1 Step 1: construct (initial) fuzzy direct-relation matrix

Experts make sets of the pairwise comparisons in terms of influence and direction within necessary criteria from $\tilde{A}$, whose TFN$\tilde{a}_{ij} = \left(l_{ij}, m_{ij}, u_{ij}\right)$ represents the degree to which the element i affects the element j.

2.2.2 Step 2: acquire fuzzy normalized direct-relation matrix

Establish normalized fuzzy direct-relation matrix $\tilde{\mathrm{X}}$ obtained from matrix $\tilde{\mathrm{A}}$ by using Eq. (3):

$$\tilde{X} = s \times \tilde{A}$$
$$\text{where } s = 1/max_{1\le i\le n}\sum_{j=1}^{n} u_{ij} \text{ and } \tilde{a}_{ij} = \left(l_{ij}, m_{ij}, u_{ij}\right). \tag{3}$$

2.2.3 Step 3: acquire fuzzy total-relation matrix

After establishing the normalized direct-relation matrix $\tilde{X}$, the fuzzy total-relation matrix $\tilde{T}$ can be established using the following equations, in which I is denoted as the identity matrix.

Let $\tilde{x}_{ij} = \left(l_{ij},\ m_{ij},\ u_{ij}\right)$ be the element of matrix $\tilde{X}$. It is necessary to define three crisp matrices, whose elements are extracted from $\tilde{X}$ as shown in Eqs. (4) and (5) [46]:

$$X_l = \begin{bmatrix} 0 & l_{12} & \cdots & l_{1n} \\ l_{21} & 0 & \cdots & l_{2n} \\ & \vdots & & \\ l_{n1} & l_{n2} & \cdots & 0 \end{bmatrix}, \quad X_m = \begin{bmatrix} 0 & m_{12} & \cdots & m_{1n} \\ m_{21} & 0 & \cdots & m_{2n} \\ & \vdots & & \\ m_{n1} & m_{n2} & \cdots & 0 \end{bmatrix},$$
$$X_u = \begin{bmatrix} 0 & u_{12} & \cdots & u_{1n} \\ u_{21} & 0 & \cdots & u_{2n} \\ & \vdots & & \\ u_{n1} & u_{n2} & \cdots & 0 \end{bmatrix} \tag{4}$$

According to crisp case, we define the fuzzy total-relation matrix $\tilde{T}$ based on the following equation:

$$\begin{aligned} \tilde{T} &= \tilde{X} + \tilde{X}^2 + \cdots \tilde{X}^k = \tilde{X}\left(I + \tilde{X} + \tilde{X}^2 + \cdots \tilde{X}^{k-1}\right) \\ &= \tilde{X}\left(I + \tilde{X} + \tilde{X}^2 + \cdots \tilde{X}^{k-1}\right)\left(I - \tilde{X}\right)\left(I - \tilde{X}\right)^{-1} \\ &= \tilde{X}\left(I - \tilde{X}\right)^{-1}, \ when \lim_{k\to\infty} \tilde{X}^k = [0]_{nxn} \end{aligned} \tag{5}$$

Here, if $\tilde{T} = \begin{bmatrix} \tilde{t}_{11} & \tilde{t}_{12} & \cdots & \tilde{t}_{1n} \\ \tilde{t}_{21} & \tilde{t}_{22} & \cdots & \tilde{t}_{2n} \\ & \vdots & & \\ l_{n1} & l_{n2} & \cdots & 0 \end{bmatrix}$ and $\tilde{t}_{ij} = \left(l''\right)_{ij}, m''$, then

Matrix $\left(l'_{ij}\right) = X_l\left(I - X_l\right)^{-1}$

Matrix $\left(m''\right)_{ij} = X_m\left(I - X_m\right)^{-1}$

Matrix $\left(u''\right)_{ij} = X_u\left(I - X_u\right)^{-1}$

2.2.4 Step 4: obtain inner dependence matrix, and obtain network relation map

In order to obtain the values of inner dependence between elements within the same cluster, elements of matrix $\tilde{T}$ are defuzzified based on the following Eq. (6) [60]:

$$dF_{ij} = \frac{\left((u_{ij} - l_{ij}) + (m_{ij} - l_{ij})\right)}{3} + l_{ij} \tag{6}$$

The sum of rows and the sum of columns is represented as vectors d and r, respectively, in the total influence matrix T, as in Eq. (7):

$$T = [t_{ij}], i, j \in \{1, 2, \ldots, n\}$$
$$d = (d_i)_{n\times 1} = \left[\sum_{j=1}^{n} t_{ij}\right]_{n\times 1}; r = (r_j)'_{n\times 1} = \left[\sum_{i=1}^{n} t_{ij}\right]'_{n\times 1} \tag{7}$$

$d + r$ represents the degree of importance (effect) that the criterion plays in the entire system, with a higher value signifying a greater effect. $d - r$ represents the causal relations among the criteria, with a higher value indicating that the criteria are the causes of other criteria, and a lower one indicating that they are the results of other criteria [59]. The network relation map (NRM) can be acquired by mapping the dataset of ($d + r$, d - r) where the horizontal axis is $d + r$ and the vertical axis is $d - r$. In practice, to reduce the complexity of the NRM, the decision maker sets a threshold value for the influence level to filter out minor effects. When the threshold value and the relative NRM have been decided, the NRM can be drawn accordingly [52].

2.3 Fuzzy ANP

Saaty proposed ANP as a new MCDM method to overcome the problems of interdependence and feedback among criteria and alternatives in decision-making processes through a "supermatrix" approach [39,40]. The ANP is a general form of the analytic hierarchy process (AHP), which extends the hierarchy relation of MCDM to a network structure [35]. ANP imposes a network that replaces the single-direction relationships of AHP with dependence and feedback [39]. ANP uses ratio scale measurements based on pairwise comparisons, and models a decision problem using a systems-with-feedback approach. By pairwise comparisons, ANP derives weights and priorities of criteria based on relative importance and reaches its final goal through judgement of alternatives. Using a supermatrix approach, ANP synthesizes the outcome of dependence and feedback within and between clusters of elements (criteria) [58]. Figure 5 shows the supermatrix representation of a hierarchy with four levels. The vector W_{21} represents the impact of the goal on the factors, the vector W_{32} represents the impact of the factors on each of the sub-factors, the vector W_{43} represents the impact of the sub-factors on each of the alternatives, and I is the identity matrix. However, the influence of alternatives on sub-factors, influence of sub-factor on upper level factors and influence of factors on decision goal are also able to be

$$W = \begin{matrix} \\ Goal\ (G) \\ Factor(F) \\ Sub\ Factor(SF) \\ Alternatives\ (A) \end{matrix} \begin{bmatrix} G & F & SF & A \\ 0 & 0 & 0 & 0 \\ W_{21} & 0 & 0 & 0 \\ 0 & W_{32} & 0 & 0 \\ 0 & 0 & W_{43} & 0 \end{bmatrix}$$

Fig. 5 Decision hierarchy in supermatrix

evaluated, since, the difference between AHP and ANP lies in the fact that ANP imposes an interrelation among factors and sub factors by allowing dependence and feedback.

As indicated in the previous section, human judgments on preferences are often unclear and hard to estimate using exact numerical values. However, qualitative judgement is needed in order to evaluate relative importance among various security requirements. Thus, the use of fuzzy logic is justified in evaluating the security assessment of the IoT, as it mitigates the problems of vagueness and imprecision.

Furthermore, a hybrid MCDM combining ANP and DEMATEL to solve the dependence and feedback problems has been successfully used in various fields [3,7,9,46,52,59,60]. In traditional ANP approaches, each criterion in a column is divided by the number of clusters (upper level criteria) so that each column adds up to unity, which implies that each cluster has the same weight. However, in the real world, there are different degrees of influence among the clusters of factors and criteria. Thus, the assumption of equal weights for each cluster to obtain the weighted supermatrix is unrealistic and needs to be improved. This study uses the results from DEMATEL to improve the normalization process in ANP. Here, DEMATEL is used not only to construct the interrelations between factors/criteria in building an NRM but also to improve the overall normalization process of ANP [58].

Equations and calculation steps of fuzzy ANP are described below [7]:

2.3.1 Step 1: construct fuzzy pairwise comparison matrix

Based on pairwise comparisons, fuzzy comparison matrix $\tilde{A}'$ is constructed as:

$$\tilde{A}' = \begin{bmatrix} \tilde{a}'_{11} & \tilde{a}'_{12} & \cdots & \tilde{a}''_{1n} \\ \tilde{a}'_{21} & \tilde{a}''_{22} & \cdots & \tilde{a}''_{2n} \\ & \vdots & & \\ \tilde{a}''_{n1} & \tilde{a}''_{n2} & \cdots & \tilde{a}''_{nn} \end{bmatrix},$$

where $\tilde{a}''_{ij} = (l'')\,ij$ indicates the importance among the compared criteria (importance of i over j), and where $i = j = 1, 2, \ldots, n$.

2.3.2 Step 2: calculate weights of criteria

Using priority vectors from each pairwise comparison matrix, complete the various supermatrix submatrices. Estimate triangular fuzzy priorities $\bar{w}_k$, where $k = j = 1, 2, \ldots, n$ from the judgment matrix.

There are many fuzzy AHP methods for calculating weights to be used in the supermatrix of fuzzy ANP, as proposed by various researchers [6,8,11,14,24,29,53]. These methods are systematic approaches to the alternative selection and justification problem using the concepts of fuzzy set theory and hierarchical structure analysis [52,61].

In this study, the logarithmic least-squares method, as shown in Eq. (8), is used for calculating the overall weights of criteria [34,36,50,51]:

$$\tilde{W}_k = \left(w_k^l, w_k^m, w_k^u\right), \quad k = 1, 2, \ldots, n$$
$$\text{where } w_k^s = \frac{(\prod_{i=1}^{n} a_{kj}^s)^{1/n}}{\sum_{i=1}^{n}(\prod_{i=1}^{n} a_{ij}^m)^{1/n}}, \quad s \in \{l, m, u\}$$
$$\text{for } 0 < \alpha \leq 1 \text{ and all } i, j = 1, 2, \ldots, n, \ j = 1, 2, \ldots, n. \tag{8}$$

2.3.3 Step 3: consistency test

In order to control the result of the method, the consistency ratio for each of the matrices and the overall inconsistency for the hierarchy are calculated as follows:

$$CR = CI/RI$$
$$\text{where } CI = \frac{i_{max} - n}{n - 1}$$

i_{max} is the Perron root or principal eigenvalue of matrix $\tilde{A}$ [16]. *RI* is the value for matrices of various sizes [39]. Here, n = 2,…,8, and *RI* is 0.00; 0.58; 0.90; 1.12; 1.24; 1.32; 1.41, respectively. The consistency ratio (*CR*) is used to directly estimate the consistency of the pairwise comparisons and should be less than 0.10 to be considered as acceptable; otherwise, they are not acceptable. In this study, the inconsistency ratios for all the comparison matrices were calculated for the mean values of the fuzzy numbers. Because the lower and upper values provide flexibility for human judgments, they are not expected to have rigid consistency.

2.3.4 Step 4: obtain the weights and priorities of criteria from the limit supermatrix

By entering the priorities found by fuzzy DEMATEL and fuzzy ANP into the appropriate columns, an initial supermatrix can be constructed. Each of the columns may be normalized by dividing each weight in the column by the sum of that column. By multiplying the weight of the criteria to the initial supermatrix, the weighted supermatrix is acquired. The final step in the process is to obtain a priority ranking for each of the alternatives. To derive the overall priorities of elements, the normalized supermatrix is raised to limiting powers, and thus the cumulative influence of each element on every other element with which it interacts is obtained [35].

3 Empirical analysis

A primary focus of this research is to derive a security assessment framework for the IoT environment. For this purpose, a hybrid MCDM model combining fuzzy DEMATEL and fuzzy ANP is proposed to investigate internal relations among various security criteria (or requirements) and to analyze overall weights and priorities for those criteria. To determine and evaluate the security assessment framework, we organized a committee of 38 expert members who each had over 8 years of experience in mobile security and IS architecture and are now working as IoT security experts in various fields.

Most of the committee members (32) are taking part in the "Vitathon Project," a national IoT project in Korea, working as project managers in the IoT security and architecture design section [30]. The overall aim of the project is to revitalize the national economy by implementing various types of ICT, especially IoT, in a myriad of traditional industries and services (e.g., agriculture, healthcare, SOC, and education). It is a 3-year project with revenues of 100 billion won (approximately US$100 million per year and one of the biggest IoT projects in Korea. Some of the expert members are either professors (2) or senior researchers (2) who have participated in the working group for national IoT roadmap planning as advisory committee members, and the remainders (2) are researchers from the Korea Internet Security Agency (KISA) who are managing and conducting an IoT security-related project. The background of the expert members verifies their profound knowledge and understanding of the IoT security field as well as their capability to make decisions and evaluate the security assessment framework for IoT service. Most of the expert evaluations were gathered by face-to-face meetings, and a few were collected by e-mail. The expert evaluations were conducted two times: the first evaluation was for internal relations among security criteria based on fuzzy DEMATEL, and the second involved pairwise comparisons based on fuzzy ANP.

Experts' evaluation was conducted to collect a pair-wise comparison matrix from the four evaluation criteria and 19 sub-criteria based on two phases of analysis. The first phase of the analysis is to investigate the interrelations of the security criteria according to the architectural view point. The

Table 3 Initial fuzzy direct-relation matrix among criteria

	C1	C2	C3	C4
C1	(0, 0, 0)	(6.19, 8.22, 8.76)	(1.48, 2.12, 4.64)	(3.18, 5.21, 8.64)
C2	(0, 0, 0)	(0, 0, 0)	(2.76, 4.96, 6.94)	(3.06, 5.18, 8.22)
C3	(0.42, 2.18, 4.26)	(6.54, 8.08, 8.86)	(0, 0, 0)	(3.12, 5.26, 8.72)
C4	(0.64, 0.89, 1.89)	(0.61, 0.72, 1.62)	(0.28, 0.36, 0.98)	(0, 0, 0)

Table 4 Initial fuzzy direct-relation matrix among sub-criteria of system dependability (C1)

	c11	c12	c13	c14	c15	c16
c11	(0, 0, 0)	(1.46, 2.68, 4.48)	(3.68, 6.21, 8.01)	(0.26, 0.78, 1.66)	(0.98, 1.92, 3.05)	(4.94, 6.89, 8.88)
c12	(3.06, 5.26, 7.66)	(0, 0, 0)	(2.58, 4.64, 6.89)	(0.46, 0.88, 1.69)	(1.21, 2.12, 3.64)	(0.48, 1.64, 3.01)
c13	(0.22, 0.64, 1.6)	(1.46, 2.64, 4.46)	(0, 0, 0)	(0.18, 0.46, 0.98)	(2.36, 4.26, 6.78)	(0.22, 0.66, 1.61)
c14	(0.86, 1.64, 3.01)	(1.28, 2.12, 3.89)	(3.76, 5.89, 8.20)	(0, 0, 0)	(2.42, 4.89, 6.96)	(0.19, 0.21, 0.99)
c15	(2.22, 4.26, 6.26)	(1.86, 3.68, 5.01)	(4.72, 6.77, 8.44)	(0.52, 1.01, 1.89)	(0, 0, 0)	(1.47, 2.68, 4.46)
c16	(5.16, 7.66, 8.61)	(0.22, 0.32, 1.08)	(3.66, 5.68, 7.88)	(0.22, 0.64, 1.12)	(1.89, 3.12, 5.06)	(0, 0, 0)

Table 5 Initial fuzzy direct-relation matrix among sub-criteria of service layer (C2)

	c21	c22	c23	c24	c25	c26
c21	(0, 0, 0)	(1.46, 2.66, 4.46)	(0.87, 1.68, 2.87)	(5.98, 7.89, 8.88)	(5.94, 7.66, 8.64)	(4.99, 6.96, 8.54)
c22	(2.01, 4.06, 6.04)	(0, 0, 0)	(6.77, 8.96, 9.00)	(2.99, 5.06, 7.46)	(4.63, 6.07, 8.02)	(1.11, 2.02, 4.1)
c23	(3.08, 5.44, 7.62)	(6.77, 8.96, 9.00)	(0, 0, 0)	(1.46, 2.68, 4.49)	(5.99, 7.88, 8.88)	(1.25, 2.32, 4.33)
c24	(6.22, 8.26, 8.66)	(0.78, 1.77, 3.18)	(1.47, 2.78, 4.67)	(0, 0, 0)	(4.87, 6.98, 8.21)	(6.78, 8.98, 9,00)
c25	(1.45, 2.68, 4.49)	(0.62, 1.69, 3.02)	(0.95, 1.98, 3.29)	(0.94, 1.96, 3.28)	(0, 0, 0)	(3.00, 5.06, 7.12)
c26	(6.34, 8.66, 8.72)	(0.61, 1.69, 2.98)	(0.66, 1.86, 3.26)	(5.98, 7.88, 8.87)	(5.88, 7.67, 8.66)	(0, 0, 0)

experts were given the first set of questionnaires which consist of a scale of 1, 3, 5, 7, and 9 representing the range from "has no influence" to "has extremely high influence", with respondents proposing the degree of direct influence that each criteria on other criteria. The data from the first questionnaires were then analyzed using fuzzy DEMATEL method. The second phase of the analysis was to investigate the weights of importance/preference of the sub-criteria based on the above-mentioned experts' judgements. Here, also questionnaires which consist of a 5 fuzzy scale of 1, 3, 5, 7, and 9 representing the range from "equally important/preferred" to "extremely important/preferred" were given to the experts. The corresponding data were used to analyze weights of each criteria and sub-criteria using ANP method. After linguistic judgements on the relations and importance of each criteria/sub-criteria were obtained, the linguistic judgements were converted in to TFN by using Table 2. These linguistic judgements were aggregated to crisp values which represent the degree to which evaluation criteria have direct impacts on each other (for DEMATEL) and the degree to which evaluation criteria and sub-criteria have importance on each other (for ANP). The initial direct-relation matrix (Tables 3, 4, 5, 6, 7) is obtained and the total-relation matrix (Tables 8, 9, 10, 11, 12, 13) is obtained by normalize initial direct relation. Finally, overall weights of each criteria and sub-criteria were obtained by limiting supermatrix (Fig. 8). Detailed explanation on each step of analysis is as illustrated in following sections.

3.1 Internal relations among security criteria

As mentioned, the fuzzy DEMATEL method is applied to analyze internal relations among security requirements. The experts' judgements were collected, and an initial fuzzy direct-relation matrix was obtained. The result of the initial fuzzy direct-relation matrix among criteria is provided in Table 3. Tables 4, 5, 6 and 7 present the result of the initial fuzzy direct-relation matrices among the sub-criteria of criteria C1–C4.

Next, the values in the fuzzy direct-relation matrix were transferred into the normalized direct-relation fuzzy matrix. After obtaining the normalized direct-relation fuzzy matrix, the fuzzy total-relation matrix is acquired. The final total-relation matrices among criteria and sub-criteria are produced through the defuzzification process.

Table 6 Initial fuzzy direct-relation matrix among sub-criteria of network layer (C3)

	c31	c32	c33	c34
c31	(0, 0, 0)	(0.43, 2.19, 4.66)	(3.18, 5.21, 8.64)	(3.06, 5.18, 8.51)
c32	(0.66, 1.01, 3.46)	(0, 0, 0)	(6.01, 8.06, 9)	(2.82, 4.88, 6.88)
c33	(1.06, 3.12, 5.78)	(3.21, 6.88, 8.78)	(0, 0, 0)	(3.22, 5.89, 8.78)
c34	(3.18, 5.69, 8.76)	(2.67, 4.96, 6.96)	(3.02, 5.18, 8.51)	(0, 0, 0)

Table 7 Initial fuzzy direct-relation matrix among sub-criteria of privacy (C4)

	c41	c42	c43
c41	(0, 0, 0)	(2.30, 4.64, 6.89)	(3.82, 6.46, 8.24)
c42	(1.14, 3.26, 6.02)	(0, 0, 0)	(3.02, 5.88, 8.12)
c43	(3.01, 5.26, 7.86)	(4.44, 6.67, 8.8)	(0, 0, 0)

Table 8 Total-relation matrix among criteria after defuzzification

	c1	c2	c3	c4	d	$d+r$	$d-r$
c1	0.12	0.82	0.45	0.81	2.20	2.72	1.68
c2	0.10	0.29	0.42	0.61	1.42	3.49	−0.66
c3	0.22	0.81	0.30	0.79	2.12	3.39	0.85
c4	0.09	0.16	0.10	0.12	0.46	2.78	−1.86
r	0.52	2.08	1.27	2.32			

The results of the total-relation matrix among criteria and among sub-criteria after defuzzification are shown in Tables 8, 9, 10, 11 and 12. A thread value of 0.79 is applied to the result of the total-relation matrix among criteria, whereas a thread value of 0.9 is applied to the result of the total-relation matrix among sub-criteria.

The NRMs were derived by mapping the dataset of $(d+r, d-r)$ where the horizontal axis $d+r$ represents the degree of the effect and the vertical axis d-r represents the direction of the effect. The higher the value of $d+r$, the greater effect. A positive value of $d-r$ indicates that the criteria are the causes of other criteria, and a negative value indicates that the criteria are affected by other criteria. In NRM, dotted lines denote that the threshold value was not achieved, and double arrows designate mutual effects between two criteria.

As shown in Table 8 and Fig. 6, System Dependability (C1) and Network Layer (C3) have positive $d-r$ values, and are thus core areas of security that affect other security components. Service Layer (C2) and Privacy (C4) are both affected by all of the other dimensions. This result illustrates that security measures should be more focused at the Service Layer (C2), for it has the highest $d+r$ value (with a positive $d-r$ value). Moreover, security measures in the Network Layer (C3) play key role, affecting other dimensions of security components (Fig. 6).

Table 9 Total-relation matrix among sub-criteria of system dependability (C1) after defuzzification

	c11	c12	c13	c14	c15	c16	d	$d+r$	$d-r$
c11	0.88	0.73	1.49	0.25	0.88	0.98	5.20	10.39	0.01
c12	0.92	0.52	1.21	0.23	0.75	0.65	4.27	8.02	0.53
c13	0.52	0.49	0.69	0.15	0.63	0.41	2.88	10.42	−4.661
c14	0.74	0.63	1.24	0.18	0.85	0.54	4.17	5.47	2.88
c15	0.99	0.76	1.47	0.26	0.75	0.77	4.99	9.74	0.25
c16	1.13	0.63	1.45	0.23	0.90	0.69	5.02	9.07	0.98
r	5.19	3.74	7.54	1.29	4.74	4.04			

Table 10 Total-relation matrix among sub-criteria of service layer (C2) after defuzzification

	c21	c22	c23	c24	c25	c26	d	$d+r$	$d-r$
c21	1.10	0.67	0.66	1.24	1.53	1.29	6.47	13.37	−0.43
c22	1.18	0.63	0.88	1.13	1.49	1.12	6.43	10.31	2.55
c23	1.21	0.86	0.65	1.07	1.52	1.12	6.42	10.40	2.44
c24	1.37	0.67	0.71	1.07	1.57	1.37	6.74	13.15	0.34
c25	0.73	0.41	0.43	0.66	0.76	0.77	3.75	12.14	−4.63
c26	1.33	0.63	0.65	1.24	1.53	1.10	6.48	13.24	−0.27
r	6.91	3.87	3.98	6.40	8.38	6.75			

Table 11 Total-relation matrix among sub-criteria of network layer (C3) after defuzzification

	c31	c32	c33	c34	d	$d+r$	$d-r$
c31	1.70	2.25	2.86	2.61	9.42	17.24	1.60
c32	1.88	2.31	3.19	2.76	10.14	20.08	0.19
c33	2.05	2.70	2.97	2.92	10.63	22.93	−1.67
c34	2.20	2.68	3.28	2.72	10.88	21.88	−0.12
r	7.82	9.95	12.30	11.00			

Table 12 Total-relation matrix among sub-criteria of privacy (C4) after defuzzification

	c41	c42	c43	d	$d+r$	$d-r$
c41	2.21	2.91	3.04	8.16	15.20	1.12
c42	2.19	2.35	2.71	7.24	15.65	−1.17
c43	2.64	3.15	2.85	8.64	17.23	0.04
r	7.03	8.41	8.59			

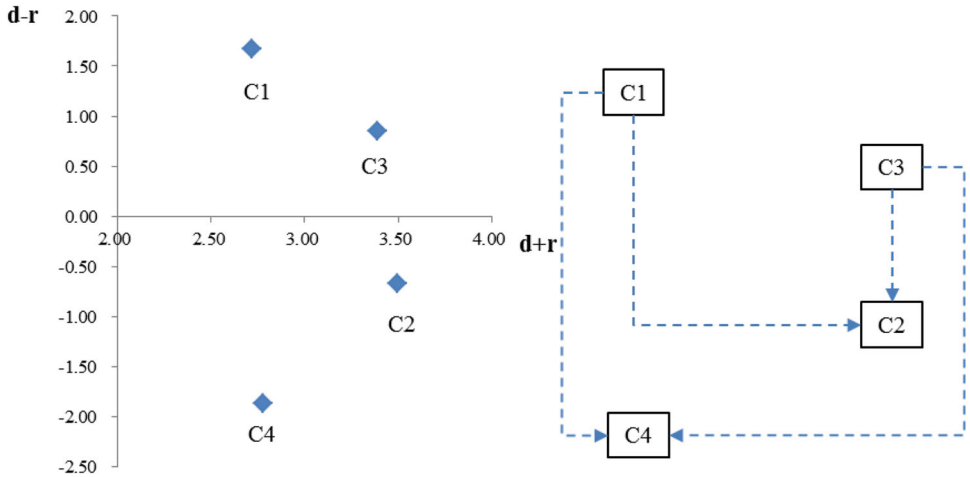


Fig. 6 The NRM of the main criteria

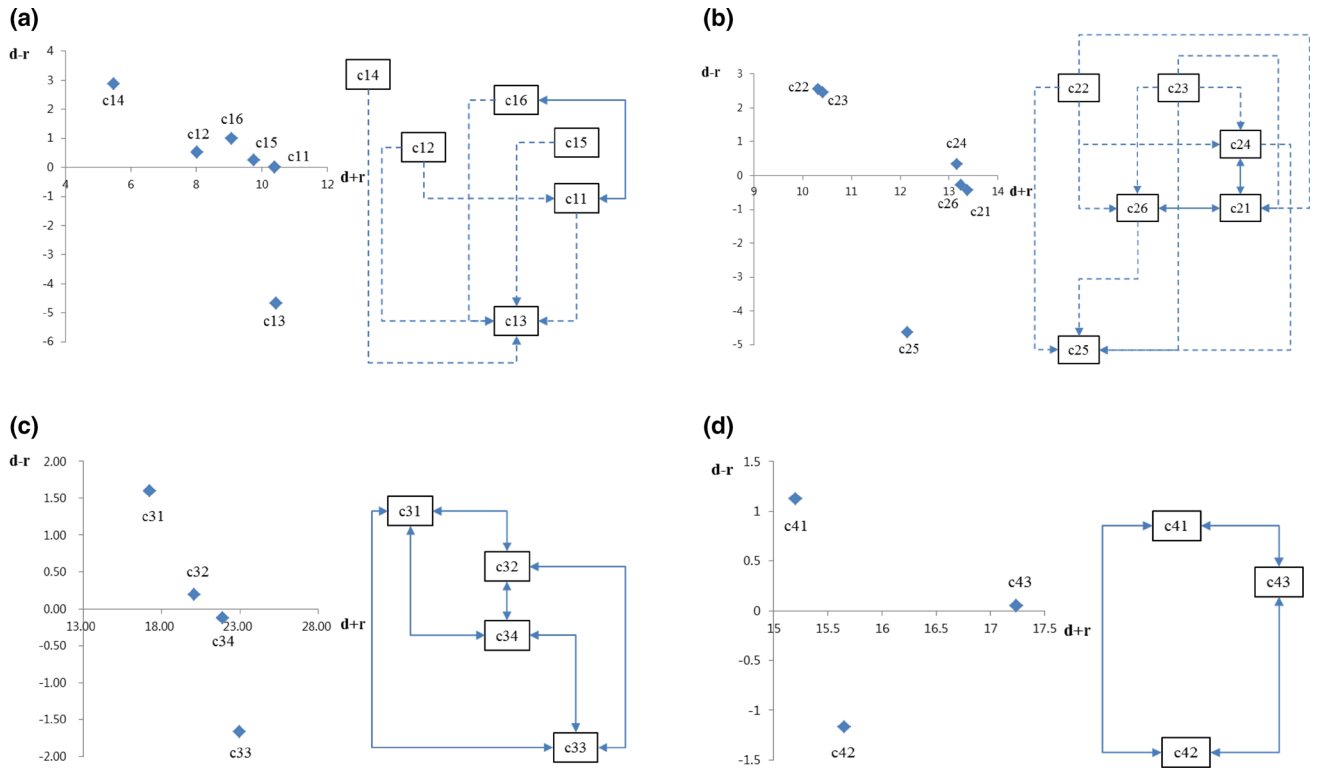


Fig. 7 The NRM for sub-criteria. (a) The NRM for Sub-criteria of System Dependability. (b) The NRM for Sub-criteria of Service Layer. (c) The NRM for Sub-criteria of Network Layer. (d) The NRM for Sub-criteria of Privacy

Figure 7 presents the NRMs for sub-criteria of System Dependability (a), Service Layer (b), Network Layer (c) and Privacy (d). Regarding System Dependability (C1), Availability (c11) has the highest $d + r$ value and the greatest effect among criteria, and Trust (13) is the largely affected by other security elements. This result is in line with that of causal relations in Service Level (C2). Service-Level Trust (c25) is alone at the bottom of the diagram with a negative $d - r$ value. Thus, we can conclude that trust is rather affected by the designs of other security mechanisms and elements. Moreover, Availability (c21) in Service Layer (C2) security has the highest $d + r$ value, meaning it has the greatest importance in service-level security. However, in Network Layer (C3), Confidentiality (c33) has a higher $d + r$ value than Availability (c34) does. Regarding network perspective, Integrity (c31) and Anonymization (c33) affect other security elements, whereas Confidentiality (c33) and Availability (c34) are affected by other security elements. In Privacy (C4),

Privacy Protection toward Users (c43) has the highest $d + r$ value, meaning it has a higher degree of effect than do Privacy Protection in Infrastructure (c41) and Privacy Protection in Service (c42).

3.2 Weights and priorities of security criteria

After calculations in fuzzy DEMATEL are finished, the fuzzy ANP approach is implemented to analyze the weights of importance among security requirements. Using pairwise comparisons, relations between elements (sub-criteria) belonging to different criteria (i.e., the outer dependencies) are established. Consistency of judgements is checked, and the CR value of all experts' judgements was less than 0.10, which demonstrates that all judgements are acceptable to use in making final comparisons. The relative weights of elements are obtained, and the initial supermatrix is formed by entering the priorities found in fuzzy DEMATEL (see Table 13). By raising the supermatrix to the power $2p + 1$ (where p is a sufficiently large number), the matrix is converging and thus forming the final limit supermatrix.

The result of the supermatrix is used to derive the overall weights and priorities among security requirements for the IoT environment are derived. As in the limit supermatrix in Table 14 and Fig. 8, Availability (c21) in the Service Layer (C2) is the most important consideration in the IoT environment. After that, the priorities are Trust (c25) in the Service Layer (C2) and Availability (c11) in System Dependency (C1). Traditional security mechanisms have put much focus on infrastructures, including system platform and network. However, much of effort is needed in the service layer, which is closer to end users.

4 Conclusion

This study applied a hybrid MCDM approach in order to propose a security assessment framework for the IoT environment. We defined the security requirements to be considered in the IoT context and grouped them into four logical components based on previous literature. The combined fuzzy DEMATEL and fuzzy ANP approaches used in this study offered a more precise and accurate analysis by integrating interdependent relations among criteria. As the complexity of the fuzzy ANP grows exponentially with the number of security requirements in the framework, the problem is simplified by using the fuzzy DEMATEL method for determining the degree of the inner dependencies between the security requirements [46]. What makes this paper stand out from other research in the field, in addition to a newly proposed hybrid MCDM model, is that it provides an approach for strategic decision regarding security assessment problem. The huge number of heterogeneous things being connected in IoT network raises serious challenges in terms of security for several reasons. The heterogeneous nature makes conventional security count measures inefficient because it requires different functionalities depending on the context of applications. It also complicates update and patch procedures to the point of increasing the window of vulnerability to a specific attack [13]. Moreover most of the things in IoT are characterized by limited-capabilities in terms of both energy and computing resources and thus, they cannot implement complex schemes supporting security. Security measures should further take into account the limited-capabilities of things and heterogeneous nature. Security mechanisms which provide different measures and different security resources based on IoT context should be developed, with particular focus on possible spoofing and DoS/DDoS attacks. By providing a practical guidance on how to allocate security resources within the security elements, security assessment framework from this study would help decision makers in IoT security field to better cope with diversified attacks in IoT environment.

In order to facilitate widespread adoption of IoT applications, a technically sound solution that guarantees users' security and privacy is needed. Public acceptance of the IoT will happen only when strong security and privacy solutions are in place. Therefore, security and privacy should be integrated into IoT system design from the beginning stages. There are countless security considerations that need to be taken into account. All common aspects of conventional IS security requirements must be considered from the initial stage of IoT system development.

We anticipate that security issues in the IoT environment will soon become a challenging task, as the IoT paradigm will bridge the physical world with the Internet at some point in the future. The increasing complexity of systems will multiply the number of security challenges. It may sound like a perfect solution to put all of these security mechanisms in the system and introduce devices armed with hundreds of security add-ons. Unfortunately, this is not the answer to the security alerts of the IoT environment, as most devices at the end-point are small sensors or mobile devices that have relatively little computing capacity. According to our analysis result, the most important security area is the service layer. In particular, ensuring service availability is a top priority in the IoT environment. However, much of the concentration is still on infrastructure security for networks and systems. Looking at security and privacy from an infrastructure perspective is not enough. Service availability and trust in the application itself are necessary conditions to ensure user confidence. Security is always one of the most concerning issues for the digitalized society [41].

We believe that our hybrid MCDM model would be very useful for security assessment of IoT service, especially for the design of architecture and service implementation, as it

Table 13 Unweighted supermatrix

	c11	c12	c13	c14	c15	c16	c21	c22	c23	c24	c25	c26	c31	c32	c33	c34	c41	c42	c43
c11	0.000	0.343	0.307	0.000	0.000	0.000	0.174	0.000	0.000	0.000	1.000	0.000	0.512	0.222	0.151	0.598	0.000	0.286	0.000
c12	0.267	0.000	0.000	0.000	0.463	0.000	0.169	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.166	0.402	0.000	0.000	0.000
c13	0.312	0.306	0.000	0.000	0.537	0.608	0.122	0.409	0.000	1.000	0.000	0.000	0.000	0.264	0.181	0.000	0.000	0.000	0.000
c14	0.000	0.000	0.000	0.000	0.000	0.000	0.116	0.591	0.000	0.000	0.000	0.000	0.000	0.275	0.189	0.000	1.000	0.437	0.000
c15	0.421	0.000	0.351	0.286	0.000	0.392	0.216	0.000	0.000	0.000	0.000	1.000	0.488	0.000	0.146	0.000	0.000	0.277	0.000
c16	0.000	0.351	0.342	0.714	0.000	0.000	0.204	0.000	0.000	0.000	0.000	0.000	0.000	0.240	0.167	0.000	0.000	0.000	0.000
c21	1.000	1.000	0.206	0.000	0.250	1.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.213	0.000	0.000	0.000	0.000
c22	0.000	0.000	0.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000	1.000	0.225	0.000	0.000	0.000	0.000	1.000	1.000	0.000
c23	0.000	0.000	0.232	0.000	0.000	0.000	0.000	0.000	0.000	0.685	0.000	0.253	0.500	0.000	0.277	0.000	0.000	0.000	0.000
c24	0.000	0.000	0.309	0.000	0.250	0.000	0.000	0.000	0.404	0.000	0.000	0.523	0.500	0.000	0.510	0.000	0.000	0.000	0.000
c25	0.000	0.000	0.072	0.000	0.250	0.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
c26	0.000	0.000	0.180	0.000	0.250	0.000	0.000	1.000	0.596	0.315	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
c31	0.000	0.000	0.179	0.000	0.000	0.000	0.000	0.000	0.000	0.165	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.186
c32	0.334	0.000	0.265	0.000	0.481	0.000	0.000	0.000	0.000	0.285	0.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000	0.190
c33	0.332	1.000	0.281	1.000	0.519	0.000	0.000	0.000	0.000	0.295	0.000	0.000	0.000	0.000	0.000	0.000	0.477	0.000	0.298
c34	0.334	0.000	0.275	0.000	0.000	0.000	0.000	1.000	0.000	0.254	0.000	0.000	0.000	0.000	0.000	0.000	0.523	1.000	0.326
c41	0.000	0.000	0.000	0.488	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
c42	0.521	1.000	0.000	0.512	1.000	0.000	0.000	0.000	0.000	1.000	0.000	0.000	0.000	0.570	1.000	0.000	0.000	0.000	0.000
c43	0.479	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	1.000	0.430	0.000	0.000	0.000	1.000	0.000

Table 14 Limit supermatrix

	c11	c12	c13	c14	c15	c16	c21	c22	c23	c24	c25	c26	c31	c32	c33	c34	c41	c42	c43
c11	0.090	0.090	0.090	0.090	0.090	0.090	0.090	0.090	0.090	0.090	0.090	0.090	0.090	0.090	0.090	0.090	0.090	0.090	0.090
c12	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039	0.039
c13	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066
c14	0.028	0.028	0.028	0.028	0.028	0.028	0.028	0.028	0.028	0.028	0.028	0.028	0.028	0.028	0.028	0.028	0.028	0.028	0.028
c15	0.053	0.053	0.053	0.053	0.053	0.053	0.053	0.053	0.053	0.053	0.053	0.053	0.053	0.053	0.053	0.053	0.053	0.053	0.053
c16	0.048	0.048	0.048	0.048	0.048	0.048	0.048	0.048	0.048	0.048	0.048	0.048	0.048	0.048	0.048	0.048	0.048	0.048	0.048
c21	0.169	0.169	0.169	0.169	0.169	0.169	0.169	0.169	0.169	0.169	0.169	0.169	0.169	0.169	0.169	0.169	0.169	0.169	0.169
c22	0.040	0.040	0.040	0.040	0.040	0.040	0.040	0.040	0.040	0.040	0.040	0.040	0.040	0.040	0.040	0.040	0.040	0.040	0.040
c23	0.043	0.043	0.043	0.043	0.043	0.043	0.043	0.043	0.043	0.043	0.043	0.043	0.043	0.043	0.043	0.043	0.043	0.043	0.043
c24	0.062	0.062	0.062	0.062	0.062	0.062	0.062	0.062	0.062	0.062	0.062	0.062	0.062	0.062	0.062	0.062	0.062	0.062	0.062
c25	0.121	0.121	0.121	0.121	0.121	0.121	0.121	0.121	0.121	0.121	0.121	0.121	0.121	0.121	0.121	0.121	0.121	0.121	0.121
c26	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066	0.066
c31	0.007	0.007	0.007	0.007	0.007	0.007	0.007	0.007	0.007	0.007	0.007	0.007	0.007	0.007	0.007	0.007	0.007	0.007	0.007
c32	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032	0.032
c33	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033
c34	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033	0.033
c41	0.009	0.009	0.009	0.009	0.009	0.009	0.009	0.009	0.009	0.009	0.009	0.009	0.009	0.009	0.009	0.009	0.009	0.009	0.009
c42	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045	0.045
c43	0.016	0.016	0.016	0.016	0.016	0.016	0.016	0.016	0.016	0.016	0.016	0.016	0.016	0.016	0.016	0.016	0.016	0.016	0.016

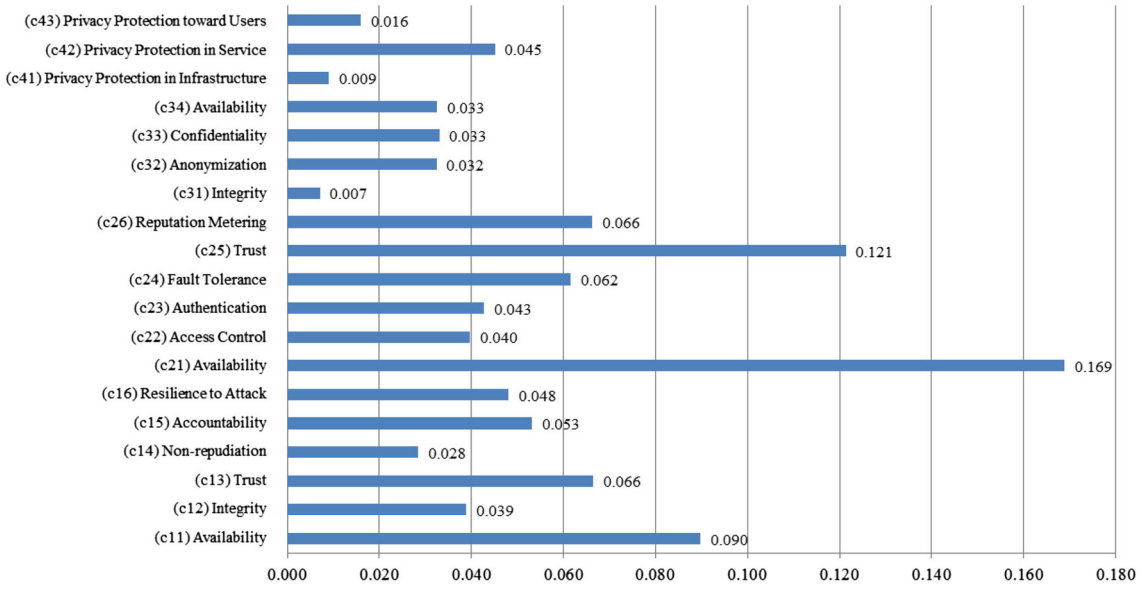


Fig. 8 Overall proprieties security requirements in IoT service

helps to make strategic decisions on how to allocate various security assets and resources to the service layer. However, further study is needed due to limitations of the study. There are two kinds of security capabilities: generic security capabilities and specific security capabilities. Generic security capabilities are independent of applications, and they include the conventional security requirements this study has investigated. On the other hand, specific security capabilities are closely coupled with application-specific requirements (e.g., mobile payment, education, and healthcare). Whereas our study focuses on generic security capabilities, deriving specific security capabilities is also an urgent issue in the field. Thus, future research should be conducted on context-specific security measures.

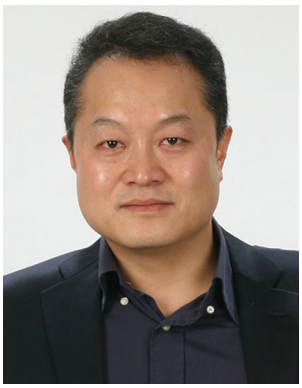
References

1. Abomhara, M., & Koien, G. M. (2014, May). *Security and privacy in the Internet of Things: Current status and open issues*. Paper presented at the 2nd international conference on privacy and security in mobile systems, Aalborg. doi:10.1109/PRISMS.2014.6970594
2. Alam, S., Chowdhury, M. M., & Noll, J. (2011). Interoperability of security-enabled Internet of things. *Wireless Personal Communications*, *61*(3), 567–586. doi:10.1007/s11277-011-0384-6.
3. Attari, M. Y. N., Bagheri, M., & Jami, E. N. (2012). A decision making model for outsourcing of manufacturing activities by ANP and DEMATEL under fuzzy environment. *International Journal of Industrial Engineering, 23*(3), 163–174. Retrieved from http://ijiepr.iust.ac.ir/browse.php?a_code=A-10-149-2&slc_lang=en&sid=1.
4. Babar, S., Mahalle, P., Stango, A., Prasad, N., & Prasad, R. (2010). Proposed security model and threat taxonomy for the Internet of things. In N. Meghanathan, et al. (Eds.), *Recent trends in network security and applications* (pp. 420–429). Berlin: Springer.
5. Bellman, R. E., & Zadeh, L. A. (1970). Decision-making in a fuzzy environment. *Management Science*, *17*(4), B-141–B-164. doi:10.1287/mnsc.17.4.B141.
6. Buckley, J. J. (1985). Fuzzy hierarchical analysis. *Fuzzy Sets and Systems*, *17*(3), 233–247. doi:10.1016/0165-0114(85)90090-9.
7. Büyüközkan, G., & Çifçi, G. (2012). A novel hybrid MCDM approach based on fuzzy DEMATEL, fuzzy ANP and fuzzy TOPSIS to evaluate green suppliers. *Expert Systems with Applications*, *39*(3), 3000–3011. doi:10.1016/j.eswa.2011.08.162.
8. Chang, D. Y. (1996). Applications of the extent analysis method on fuzzy AHP. *European Journal of Operational Research*, *95*(3), 649–655. doi:10.1016/0377-2217(95)00300-2.
9. Chen, J.-K., & Chen, I.-S. (2010). Using a novel conjunctive MCDM approach based on DEMATEL, fuzzy ANP, and TOPSIS as an innovation support system for Taiwanese higher education. *Expert Systems with Applications*, *37*(3), 1981–1990. doi:10.1016/j.eswa.2009.06.079.
10. Chen-Yi, H., Ke-Ting, C., & Gwo-Hshiung, T. (2007). FMCDM with fuzzy DEMATEL approach for customers' choice behavior model. *International Journal of Fuzzy Systems*, *9*(4), 236–246.
11. Cheng, C.-H. (1997). Evaluating naval tactical missile systems by fuzzy AHP based on the grade value of membership function. *European Journal of Operational Research*, *96*(2), 343–350. doi:10.1016/S0377-2217(96)00026-4.
12. Cirani, S., Ferrari, G., & Veltri, L. (2013). Enforcing security mechanisms in the IP-based internet of things: An algorithmic overview. *Algorithms*, *6*(2), 197–226. doi:10.3390/a6020197.
13. Covington, M. J., & Carskadden, R. (2013, June). Threat implications of the internet of things. In *2013 5th IEEE International conference on cyber conflict* (pp. 1–12).
14. Deng, H. (1999). Multicriteria analysis with fuzzy pairwise comparison. *International Journal of Approximate Reasoning*, *21*(3), 215–231. doi:10.1016/S0888-613X(99)00025-0.
15. Europol. (2014). *The Internet Organized Crime Threat Assessment*. European Cybercrime Centre (EC3). Retrieved from https://www.europol.europa.eu/iocta/2014/.

16. Forman, E. H., & Gass, S. I. (2001). The analytic hierarchy process–An exposition. *Operations Research*, *49*(4), 469–486. doi:10.1287/opre.49.4.469.11231.
17. FTC. (2015). *Internet of things: Privacy & security in a connected world*. FTC Staff Report. Retrieved from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
18. Gabus, A., & Fontela, E. (1972). *World problems, an invitation to further thought within the framework of DEMATEL*. Geneva: Battelle Geneva Research Center.
19. Gazis, V., Sasloglou, K., Frangiadakis, N., & Kikiras, P. (2012, October). *Wireless sensor networking, automation technologies and machine to machine developments on the path to the Internet of Things.* Paper presented at 16th Panhellenic conference on informatics (PCI), Piraeus. doi:10.1109/PCi.2012.64
20. Giachetti, R. E., & Young, R. E. (1997). A parametric representation of fuzzy numbers and their arithmetic operators. *Fuzzy Sets and Systems*, *91*(2), 185–202. doi:10.1016/S0165-0114(97)00140-1.
21. Guillemin, P., & Friess, P. (2009, September). *Internet of things strategic research roadmap*. The Cluster of European Research Projects. Technical Report.
22. IoT-A. (2012). *D4.2 concepts and solutions for privacy and security in the resolution infrastructure*. FP7 Integrated Project Internet of Things Architecture. Retrieved from http://www.iot-a.eu/public/public-documents/d4.2/view.
23. Karsak, E. E., & Tolga, E. (2001). Fuzzy multi-criteria decision-making procedure for evaluating advanced manufacturing system investments. *International Journal of Production Economics*, *69*(1), 49–64. doi:10.1016/S0925-5273(00)00081-5.
24. Leung, L. C., & Cao, D. (2000). On consistency and ranking of alternatives in fuzzy AHP. *European Journal of Operational Research*, *124*(1), 102–113. doi:10.1016/S0377-2217(99)00118-6.
25. Lin, C.-L., & Tzeng, G.-H. (2009). A value-created system of science (technology) park by using DEMATEL. *Expert Systems with Applications*, *36*(6), 9683–9697. doi:10.1016/j.eswa.2008.11.040.
26. Maras, M. H. (2015). Internet of Things: Security and privacy implications. *International Data Privacy Law*, *5*(2), 99–104. doi:10.1093/idpl/ipv004.
27. Mardani, A., Jusoh, A., & Zavadskas, E. K. (2015). Fuzzy multiple criteria decision-making techniques and applications–Two decades review from 1994 to 2014. *Expert Systems with Applications*, *42*(8), 4126–4148. doi:10.1016/j.eswa.2015.01.003.
28. Middleton, P., Kjeldsen, P., & Tully, J. (2013, November).*Forecast: The Internet of things, worldwide*. Stamford, CT: Gartner Research. Retrieved from https://www.gartner.com/doc/2625419/forecast-internet-things-worldwide.
29. Mikhailov, L. (2004). Group prioritization in the AHP by fuzzy preference programming method. *Computers & Operations Research*, *31*(2), 293–301. doi:10.1016/S0305-0548(03)00012-1.
30. Ministry of Science, ICT and Future Planning. (2013). Vitamin Project Initiatives for creative economy in Korea. http://www.msip.go.kr/webzine/index.do, https://www.facebook.com/vitathon
31. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497–1516. doi:10.1016/j.adhoc.2012.02.016.
32. Nedeltchev, P. (2014). *The Internet of everything is the new economy*. Cisco. Retrieved from http://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/Cisco_IT_Trends_IoE_Is_the_New_Economy.html.
33. Ning, H., Liu, H., & Yang, L. T. (2013). Cyberentity security in the Internet of Things. *Computer*, *46*(4), 46–53. doi:10.1109/MC.2013.74.
34. Önüt, S., Kara, S. S., & Işik, E. (2009). Long term supplier selection using a combined fuzzy MCDM approach: A case study for a telecommunication company. *Expert Systems with Applications*, *36*(2), 3887–3895. doi:10.1016/j.eswa.2008.02.045.
35. Park, K. C., Shin, J. W., & Lee, B. G. (2014). Analysis of authentication methods for smartphone banking service using ANP. *KSII Transactions on Internet and Information Systems (TIIS)*, *8*(6), 2087–2103. Retrieved from http://www.dbpia.co.kr/Article/3531347.
36. Ramik, J. (2007). A decision system using ANP and fuzzy inputs. *International Journal of Innovative Computing, Information and Control*, *3*(4), 825–837.
37. Raza, S., Shafagh, H., Hewage, K., Hummen, R., & Voigt, T. (2013). Lithe: Lightweight secure CoAP for the internet of things. *IEEE Sensors Journal*, *13*(10), 3711–3720. doi:10.1109/JSEN.2013.2277656.
38. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266–2279.
39. Saaty, T. L. (1996). *The analytic network process: Decision making with dependence and feedback; the organization and prioritization of complexity*. Pittsburgh, PA: RWS Publications.
40. Saaty, T. L. (2006). The analytic network process. In T. L. Saaty & L. G. Vargas (Eds.), *Decision making with the analytic network process* (pp. 1–26). Berlin: Springer.
41. Shin, D. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers*, *22*(5), 428–438.
42. Shin, D. (2014). A socio-technical framework for Internet-of-Things design: A human-centered design for the Internet of Things. *Telematics and Informatics*, *31*(4), 519–531.
43. Shin, D. (2015). Effect of the customer experience on satisfaction with smartphones: Assessing smart satisfaction index with partial least squares. *Telecommunications Policy*, *39*(8), 627–641.
44. Sun, C.-C. (2010). A performance evaluation model by integrating fuzzy AHP and fuzzy TOPSIS methods. *Expert Systems with Applications*, *37*(12), 7745–7754.
45. Syamsuddin, I., & Hwang, J. (2010, October). *A new fuzzy MCDM framework to evaluate e-government security strategy*. Paper presented at 2010 4th international conference on application of information and communication technologies, Uzbekistan.
46. Tadić, S., Zečević, S., & Krstić, M. (2014). A novel hybrid MCDM model based on fuzzy DEMATEL, fuzzy ANP and fuzzy VIKOR for city logistics concept selection. *Expert Systems with Applications*, *41*(18), 8112–8128. doi:10.1016/j.eswa.2014.07.021.
47. Tavana, M., Zandi, F., & Katehakis, M. N. (2013). A hybrid fuzzy group ANP-TOPSIS framework for assessment of e-government readiness from a CiRM perspective. *Information & Management*, *50*(7), 383–397.
48. Tseng, M.-L. (2009). Using the extension of DEMATEL to integrate hotel service quality perceptions into a cause-effect model in uncertainty. *Expert Systems with Applications*, *36*(5), 9015–9023. doi:10.1016/j.eswa.2008.12.052.
49. Turskis, Z., Zavadskas, E. K., & Peldschus, F. (2009). Multi-criteria optimization system for decision making in construction design and management. *Engineering Economics*, *61*(1), 7–17.
50. Tuzkaya, G., Ozgen, A., Ozgen, D., & Tuzkaya, U. (2009). Environmental performance evaluation of suppliers: A hybrid fuzzy multi-criteria decision approach. *International Journal of Environmental Science & Technology*, *6*(3), 477–490. doi:10.1007/BF03326087.
51. Tuzkaya, U. R., & Önüt, S. (2008). A fuzzy analytic network process based approach to transportation-mode selection between Turkey and Germany: A case study. *Information Sciences*, *178*(15), 3133–3146. doi:10.1016/j.ins.2008.03.015.

52. Uygun, Ö., Kaçamak, H., & Kahraman, Ü. A. (2014). An integrated DEMATEL and Fuzzy ANP techniques for evaluation and selection of outsourcing provider for a telecommunication company. *Computers & Industrial Engineering*,. doi:10.1016/j.cie.2014.09.014.
53. Van Laarhoven, P., & Pedrycz, W. (1983). A fuzzy extension of Saaty's priority theory. *Fuzzy Sets and Systems*, *11*(1), 199–227. doi:10.1016/S0165-0114(83)80082-7.
54. Vuković, D. (2014). Security issues in Internet of Things (IOT) related to passive RFID tags. *Facta Universitatis, Series: Automatic Control and Robotics*, *13*(2), 97–105.
55. Weber, R. H. (2010). Internet of Things-New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23–30. doi:10.1016/j.clsr.2009.11.008.
56. Wu, W.-W., & Lee, Y.-T. (2007). Developing global managers' competencies using the fuzzy DEMATEL method. *Expert Systems with Applications*, *32*(2), 499–507. doi:10.1016/j.eswa.2005.12.005.
57. Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of Network and Computer Applications*, *42*, 120–134. doi:10.1016/j.jnca.2014.01.014.
58. Yang, H.-W., & Chang, K.-F. (2012). Combining means-end chain and fuzzy ANP to explore customers' decision process in selecting bundles. *International Journal of Information Management*, *32*(4), 381–395. doi:10.1016/j.ijinfomgt.2011.11.005.
59. Yang, Y. P. O., Shieh, H. M., & Tzeng, G. H. (2013). A VIKOR technique based on DEMATEL and ANP for information security risk control assessment. *Information Sciences*, *232*, 482–500. doi:10.1016/j.ins.2011.09.012.
60. Yeh, T.-M., & Huang, Y.-L. (2014). Factors in determining wind farm location: Integrating GQM, fuzzy DEMATEL, and ANP. *Renewable Energy*, *66*, 159–169. doi:10.1016/j.renene.2013.12.003.
61. Yüksel, İ., & Dağdeviren, M. (2010). Using the fuzzy analytic network process (ANP) for Balanced Scorecard (BSC): A case study for a manufacturing firm. *Expert Systems with Applications*, *37*(2), 1270–1278. doi:10.1016/j.eswa.2009.06.002.
62. Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, *8*(3), 338–353.

Keon Chul Park is a Postdoctoral Research Fellow in the Department Interaction Science at Sungkyunkwan University. His research interests include ICT convergence, mobile security, social informatics and their implications on strategic action and regulatory reform.



Dong-Hee Shin is a Professor and former founding Chair of the Department Interaction Science at Sungkyunkwan University. As a Director of Interaction Science Research Center, he also serves as a Principal Investigator of BK21 Plus, a national research project hosted by the Ministry of Education in Korea (2013–2020).