IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 19, 2021, accepted June 21, 2021, date of publication September 20, 2021, date of current version September 24, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3104527

A Multicriteria Decision Making Taxonomy of IOT Security Challenging Factors

MUHAMMAD AZEEM AKBAR[1], AHMED ALSANAD[2], SAJJAD MAHMOOD[3,4], AND ABDULRAHMAN ALOTHAIM[2]

[1]Department of Information Technology, Lappeenranta University of Technology, 53851 Lappeenranta, Finland
[2]STC's Artificial Intelligence Chair, Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11451, Saudi Arabia
[3]Information and Computer Science Department, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia
[4]Interdiscilinary Research Center for Intelligent Secure Systems, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia

Corresponding authors: Muhammad Azeem Akbar (azeem.akbar@lut.fi) and Ahmed Alsanad (aasanad@ksu.edu.sa)

This work was supported by the Deanship of Scientific Research, King Saud University through the Vice Deanship of Scientific Research Chairs.

ABSTRACT Internet of things (IoT) is leading a new digital age. IoT is regarded as the significant frontier that can improve almost all aspect of our lives. Currently, the IoT technology faces several challenges to academic researchers and industry practitioners, mainly that related with security of data. The objective of this study is to develop a prioritization-based taxonomy of the challenging factors that could hinders the security of IoT. By conducting the literature review and questionnaire survey studies 21 challenging factors were identified that are reported in existing literature and in real-world practices. Moreover, the identified challenging factors are mapped in the core domain of IoT (i.e. smart city, smart home, smart wearable's and smart health care); and apply the fuzzy- AHP approach to rank the identified challenging factors with respect to their criticality for security of IoT technology. The application of fuzzy-AHP is novel in this research area as it is successfully applied in other domains of information technology to address the multi-criterion decision making problems. This study is contributing by providing a prioritization-based taxonomy of the IoT security challenging factors that could help the practitioners and research community to revise and develop the new strategies for the secure IoT.

INDEX TERMS Internet of Things (IoT), challenges, prioritization-based-taxonomy.

I. INTRODUCTION

During the last decade, Internet of Things (IoT) has attracted intensive attention due to a wide range of applications in industrial, biomedical observation, agriculture, smart cities, environmental monitoring and other fields. IoT describes the network of physical objects—"things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet [1]. With the rapid growth of high-speed network, IoT devices can be deployed in any suitable environment because of their undeniable value in future generation technology [2]. Though these devices can be controlled remotely in order to achieve the anticipated functionality. The data sharing among IoT devices takes place through the network which employs the standard communication protocols [3]. IoT consists of smart connected devices that varies form wearable device to large machines embedded with small sensor chips [1].

A variety of smart medical devices are either planted into the patient's body or may attach externally in order to monitor the glucose level or patient's medical condition [4]. Similarly, machines, electrical appliances i.e. air-conditioner, refrigerator, lights can also be controlled with on hand touch. Though, IoT is broad phenomena covering its domains like smart cities, smart homes, smart healthcare, industrial automation, smart transportation [5]. Industries may use IoT for its decision-making process, operational excellence, product and service innovation and for customer excellence [6]. Homes are equipped with smart devices that are interconnected with each other and to the internet enabling users to control remotely entertainment system, lighting system and electronic appliances etc [7]. In order to collect data from different sources for managing assets, reducing the congestion,

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

improving energy distribution, trash collection and air quality urban cities are equipped with smart IoT sensors [8]. It is envisioned that internet will be connected with more than 75.44 billion devices worldwide according to Statista research department and will generate more than 79.4 zettabytes of data by 2025 predicted by IDC (International Data Corporation).

Despite the evident significance of IoT and its applications in our daily life practices, the IoT devices are also prone to various security threats because of the existence of several vulnerabilities as Wireless Sensor Networks (WSNs), Machine-to-Machine (M2M) or Cyber-Physical System (CPS) have now advanced and are considered as an integral components for IoT paradigm [9], [10]. Thus, there needs to secure the entire architecture of IoT and its domains i.e. smart home, smart city, industrial automation, smart health from the attackers which may counterfeit the services provided by IoT. Since, IoT paradigm consists of several interconnected devices and heterogeneous devices that may prone to various conventional security issues related to computer networks. Furthermore, IoT devices are embedded with constrained resources that pose further challenges to IoT security since smart devices have very limited power to be employed with cryptographic algorithms [11].

Based on the given discussion, this study is conducted with the aim to develop a taxonomy of the factors that could negatively impact the security of IoT. The taxonomy will be based on the challenging factors identified during the literature survey and industrial study conducted with the experts. The key objective of the industrial study is to know the perceptions and opinions of the experts having experiences in IoT implementation in real-world environment. However, it is challenging to priorities multiple factors based on the experts' opinions that could bring vagueness and uncertainties. Quantitative prediction is challenging for humans (IoT practitioners), as they could more perfectly convey the feelings verbally (qualitatively). Therefore, in this study, we use the fuzzy AHP approach to translate the qualitative prediction of the IoT experts into quantitative prioritization values. It is a well-known approach that usually use for rating the human based multi criteria decision making problems. Fuzzy AHP approach has previously been used in different other studies.

For example, Singh and Prasher [12] evaluate the quality of services in different hospitals and rank the healthcare service quality attributes using Fuzzy AHP. That prioritization was eventually used for listing the best hospitals based on the quality of the services. In another study, Wang *et al.* [13] used fuzzy AHP approach to select the most common sustainability problems for both society and business in order to provide a framework for management and strategic planning. They mention that the framework work as a decision-making tool for the organizational management while they work on sustainability related issue. Similarly, Yucesan and Kahraman [14] identified, categorized and priorities various safety and financial risks in hydroelectric plant. They use fuzzy AHP approach to list down the risks based on their significance and present as a robust framework. Therefore, the use of fuzzy AHP approach in the above most recent articles motivated us to follow its concepts and develop the taxonomy of IoT challenging factors and their categories. This taxonomy will provide a robust framework that will assists the IoT practitioners to focus of the most critical areas towards the secure IoT.

RQ1: ''What are the important challenging factors towards the secure IoT paradigm reported in the literature and real-world practices?''

RQ2: ''What would be the prioritization based taxonomy of the investigated challenging factors?''

II. BACKGROUND AND MOTIVATIONS

Although the evident significance of IoT is undeniable, but the security and privacy issues existing in IoT devices is crucial that needs to be addressed. However, researchers have made a tremendous effort in order to cope with these challenges for the IoT environment. Some of them targets the layer-level security issue, whereas other approaches aim at providing end-to-end security for IoT. In recent years, several studies have been conducted in order to provide the blueprint of existing security and privacy threats for IoT paradigm. Alaba *et al.* [15] have discussed the threats on IoT in term of hardware, network, and application components and categorized the security threats of communication, architecture, application and data level. Granjal *et al.* [16] have identified and analyzed the existing security threats of various protocol designed for IoT. Whereas, several other studies likewise [17]–[20] have addressed and evaluated the key management and cryptographic algorithms that is suitable for IoT paradigm. Sicari *et al.* [21] have identified researchers' effort in order to address the confidentiality, privacy, access control and security with middleware for IoT systems. They also discussed various trust management, authentication, privacy, data security, and network issues. To ensure the privacy for IoT authors Tso *et al.* [22] have discussed the secure multi-party computation in order to preserve the privacy of end users by considering the attribute-based access control and credit checking techniques. Zhou *et al.* [23] identified several security issues and their existing solutions for cloud based IoT such as identity and location privacy, layer removing or adding, node compromising. Zhang *et al.* [24] discussed the security vulnerabilities in IoT devices such as authentication and authorization, privacy, light weight cryptographic techniques.

Several survey studies have also been conducted in order to highlight the existing security threats in various other domains of IoT such as, smart home, smart city, smart health and industrial automation [25], [26]. Kranenburg and Bassi [27] discussed several security threats existing in resource-constrained devices for smart homes. Kolzov *et al.* [28] identified the various security and privacy issues at different architectural level of smart home. Zaidan *et al.* [29] conducted a survey study concerning to smart home smart homes and found the security critical

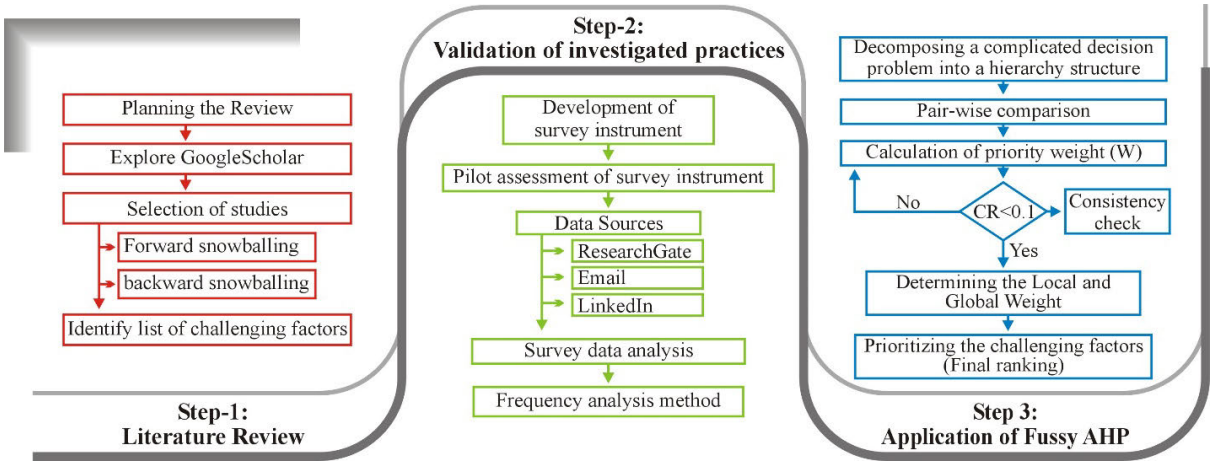

FIGURE 1. Adopted research methodology.

devices such as smart lock. Roman *et al.* [30], discussed that data and identity management, user privacy are the main challenges faced by smart- homes. Yao *et al.* [31] identified various privacy and security challenges such as identity theft, social engineering attacks, points of entry for a cyber-attack, and social network-based threats, such as, grooming and cyber-bullying.

Similarly, researches have highlighted and addressed various security and privacy threats in smart cities. Chen and Chen [32] discussed the current evolution of smart cities and identify the existing security and privacy issues pertaining to data centric. Eckhoff and Wagner [33] surveyed and highlights the nine specific technology that need privacy protection models in smart city contest. Jeong and Park [34] discussed the security and privacy threats in current smart application and highlighted the requirements for building secure and stable smart city. Several studies have been conducted in order to highlight and address the security in healthcare internet of things and industrial automation. To the best of our knowledge, there is a lack of empirical investigations on the challenging factors of IOT security. Thus this study address this gap by exploring and analyzing the IoT security challenging factors.

III. RESEARCH DESIGN

To address the objective of this research, firstly, we have conducted literature review study and investigate the challenging factors of IoT paradigm. Secondly, the empirical study was conducted aiming to get the insight of industry practitioners concerning to the identified challenges. Finally, the fuzzy-AHP approach has been applied to determine the priority level of each investigated challenge with respect to their criticality for IoT paradigm. The adopted research approaches are diagrammatically presented in Figure 1 and briefly discussed in the sub-sequent sections:

A. LITERATURE STUDY

The literature study was conducted to explore the challenging factors that could negatively impact the implementation of IoT paradigm in real-world environment. To ''conduct the literature survey, the snowball data sampling technique was adopted in which the literature were explored by applying the forward and backward snowballing. Forward snowballing refers to explore the related literature in which a particular study is used; and the backward snowballing refers to the literature cited in a particular study [35]. The sample size of the selected studies steadily increases as more references and citations are explored [35]. The relevant literature studies are listed in order to extract the factors that provide the concrete description about IoT and its security challenges. Moreover, those studies are also considered, where the factors are not explicitly discussed [36], [37], but presented the relevant IoT lesson learned and experience reports. Identifying and extracting factors from such reports are more challenging because it required complete and in-depth review [36], [37]. The literature studies are searched using the Google Scholar search engine. It provides a simple interface to broadly search the scholarly articles available on different other common digital libraries like, Springer Link, IEEE Xplore, ACM Digital Library etc. It gives us confidence that no relevant digital library has been missed. The Google Scholar search engine is explored using the keywords of the study and identify the relevant published articles. The studies selection process is mainly performed by the first three authors. However, the disagreements between investigators at any point have been settled based on the discussion and overview of all the authors. We finally shortlisted 92 studies (references list) using both forward and back snowballing technique. The studies are considered to structure this article, as well address the research questions discussed at the end of section-1.''

The first three ''authors reviewed the selected studies and develop the list of the success factors that could negatively impact the security aspect of IoT. The second review of the studies is done by the fourth and fifth authors in order to refine the results of the first review and report the missing information. Moreover, three external reviewers are invited to evaluate the interpersonal biases in the review process. The external reviewers are requested to randomly select 10 articles

and conduct the review process as performed by the authors. The interpersonal biases between the external reviewers and the authors have been assessed by performing the Kendalls coefficient of concordance (W) test. Kendalls coefficient of concordance (W) is a well-known statistical approach used to identify the level of agreement between a group of people that evaluate a set consist of n objects [38]. The range of the W assessment score is from 0 to1, where W = 0 is showing complete disagreement level between the people and W = 1 refer to complete agreement [38]. The results given in Table 1 (W = 0.84) shows that the invited external reviewers and the authors are at positive agreement level for the studies selection and data extraction process. The following code is used to perform the Kendalls coefficient of'' concordance (W):

```
library(DescTools)
IoT <- ''data.frame
(external_ex1 = c(3,3,3,4,3,4,2,3,3,2),
external_ex2 = (3,4,3,5,3,4,2,4,3,3),
external_ex3 = (3,3,4,4,3,4,1,3,3,3)
authors_abc = (2,3,3,4,2,4,3,3,2,3)
)
KendallW(IoT, TRUE)
KendallW(IoT, TRUE, test = TRUE)
)
KendallW(t(d.att[, −1]), test = TRUE)
friedman.test(y = as.matrix(d.att[, −1]), groups = d.att$id)''
```

TABLE 1. Kendall's coefficient of concordance test.

Data Set	Kendall Chi-Squared	df	Subjects	Raters	*p* value	W
IoT	35.434	14	10	3	0.001267	0.8436765

B. EMPIRICAL DATA COLLECTIONS

The identified list of challenging factors and their mapping in the core domain of IoT were further validated with industry experts via questionnaire survey approach. Questionnaire survey is an effective way to collect the data from dispersed population. Wright [39] mention that the questionnaire survey approach assists to reach the targeted population which is significant to collect the potential data.

1) SURVEY INSTRUMENT DEVELOPMENT

To collect the data from the experts, a survey instrument was developed. The survey instrument was broadly categorized in two section A and B. Section A contains the queries that related to the bibliographic information of survey respondents. Section-B of the survey instrument was further divided in two sections; which included close-ended and open-ended. In close ended, the identified challenges were mentioned and request the survey participants to rank them according to their understanding using the five-point Likert scale ''strongly agree'', ''agree'', ''neutral'', ''disagree'', and ''strongly disagree'' [40]. Finstad [41] underlined that the neutral option help to collect the unbiased data, as without neutral option, the respondents are bound to make the decision one-sided [41]–[43].

2) PILOT ASSESSMENT OF SURVEY INSTRUMENT

At first step, the questionnaire was developed with the discussion of study authors and research advisor. The pilot assessment is important to check the suitability and understandability of the variables mentioned in the questionnaire [42], [44]–[46]. In pilot assessment process, a total of three experts were participated in which once expert was invited from ''City University Hong-Kong'', two belongs to industry practices (''Virtual force'' and ''QSoft-Vietnam''). The participants were requested to analyze the questionnaire with respect to suitability of study objective and understandability of the survey participants. They analyze the whole questionnaire and suggest some modification. The major modification is regarding to the design of the questionnaire, they suggest to put all the variable in tabular form. Secondly, they suggested to add some additional questions concerning to get the strong bibliographic information of the survey participants. All the highlighted points were addressed and the updated questionnaire was used in data collection process. Appendix-A presents a sample of used questionnaire.

3) ETHICS APPROVAL

The ethical approval was obtained from research advisor committee of computer science department. Once the permission is granted, we have stated the data collection process by sending the online link of questionnaire survey to the targeted population. The collected responses were hosted at Google Drive (drive.google.com). The survey participants were requested to mark the survey questions bestowing to their knowledge. All the respondents contributed to the data collection process voluntarily and anonymous. The respondents can exist from the survey at any stage.

4) DATA SOURCES

The purpose of ''this survey was to validate the findings of literature study (i.e. challenging factor). Though, to validate the findings of literature study, the opinions of experts are important. To target the most potential population of survey study at the geographically distributed development environment, the snowball sampling strategy [42] was applied. The snowball sampling is an efficient and cost-effective way to collect the data from a physically distributed population. In snowball sampling, the participants are requested to share the survey questionnaire to their contact researchers or practitioners. The snowball sampling is an effective way to collect the data from a large and dispersed targeted population [41], [47]. Various methods were used to target the population, including personal Email, organizational Email, LinkedIn and ResearchGate. The data were collected during September-2020- to November-2020. A total of 64 responses were collected in the form of an Excel sheet. First two authors of this study

TABLE 2. Triangular fuzzy numbers.

Operation Law	Expression
Addition ($F_1 \oplus F_2$)	$(f^l_1, f^m_1, f^u_1)\oplus(f^l_2, f^m_2, f^u_2) = (f^l_1 + f^l_2,\ f^m_1 + f^m_2,\ f^u_1 + f^u_2)$
Subtraction ($F_1 \oplus F_2$)	$(f^l_1, f^m_1, f^u_1)\oplus(f^l_2, f^m_2, f^u_2) = (f^l_1 - f^l_2,\ f^m_1 - f^m_2,\ f^u_1 - f^u_2)$
Multiplication ($F_1 \oplus F_2$)	$(f^l_1, f^m_1, f^u_1)\oplus (f^l_2, f^m_2, f^u_2) = (f^l_1 * f^l_2,\ f^m_1 * f^m_2,\ f^u_1 * f^u_2)$
Division ($F_1 \oplus F_2$)	$(f^l_1, f^m_1, f^u_1)\oplus (f^l_2, f^m_2, f^u_2) = (f^l_1 / f^l_2,\ f^m_1 / f^m_2,\ f^u_1 / f^u_2)$
Inverse ($F_1 \oplus F_2$)	$(f^l_1, f^m_1, f^u_1)^{-1} = (1/f^l_1,\ 1/f^m_1,\ 1/f^u_1)$
For any real number k (kF_1)	$k(f^l_1, f^m_1, f^u_1) = k f^l_1, k f^m_1, k f^u_1$

manually reviewed all the responses. During the manual review, we found 14 incomplete responses. Though, while discussing with the research supervisor, we decided to not include the incomplete responses in the data analysis process. Finally, a total of 50 complete responses were entertained for future data analysis."

5) SURVEY DATA ANALYSIS

The "frequency analysis method is applied to analyze the collected responses statistically; the frequency analysis method is an effective way to analyze the descriptive data [48]. The frequency of occurrence and the percentage of each success factor are reported in tables. The frequency approach is useful to compare the views and values within groups of variables and across the groups of variables. To check the significance of each success factor, according to the survey respondents, the views of all the respondents are calculated and presented in the form of tables. Moreover, to check the relative importance of each success factor, the frequency of occurrence of one factor is compared with other factors. The same method is used by other researchers in several other research domains [49]–[51]."

C. FUZZY SET THEORY AND AHP

We have adopted a fuzzy analytical hierarchy process to prioritize the identified challenges of COSD process. The fundamental concepts of fuzzy sets and AHP are discussed in the section.

1) FUZZY SET

"Fuzzy set theory is an extension of classical set theory that was initially introduced by Zadeh *et al.* [52] to deal with uncertainties and vagueness in the real-world problems; and manage these ambiguities as a multi-criteria decision-making problem. The primary contribution of fuzzy set theory is to represent the vague data [53]. In the fuzzy set, a membership function is characterized which maps to objects between 0 and 1. The definitions and preliminary of the fuzzy set theory are discussed in the following sections:"

Definition: A triangular fuzzy number (TFN) F is denoted by a set (fl, fm, fu), as shown in Figure 2. The given

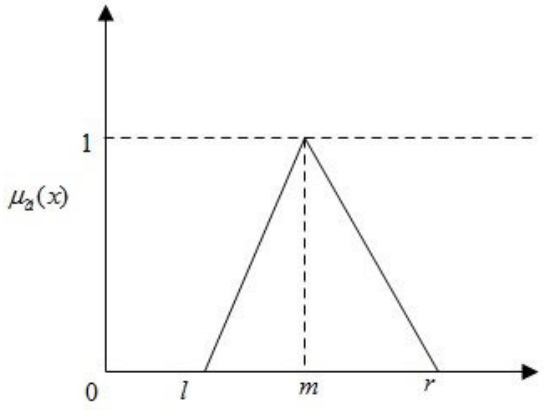

FIGURE 2. Triangular fuzzy number.

equation (1) defines the membership function μF(x) of F.

$$\mu_F(x) = \begin{cases} \dfrac{x - f^l}{f^m - f^l}, & f^l \le x \le f^m \\ \dfrac{f^u - x}{f^u - f^m}, & f^m \le x \le f^u \\ 0, & Otherwise \end{cases} \quad (1)$$

where, f^l, f^m and f^u is the crisp numbers denoting the lowest, most promising, and highest possible values respectively.

The algebraic operations for the two TFNs i.e. $\check{T}_1$, $\check{T}_2$ are given in Table 2.

2) FUZZY AHP

The analytic hierarchy process (AHP) "is one of the most powerful methods used multi-criteria decision-making problems. The main advantages of AHP are the relative ease with which it handles multiple criteria, easier to understand, and it can effectively handle both qualitative and quantitative data. The following main step of AHP method:

Step1: "*Decompose the complex decision problem into the hierarchical structure (Figure 5)*"

Step2: "*Calculate priority vector at each level of hierarchy with the help of pair-wise comparison.*"

Step3: "*Compute the consistency ratio of the pairwise comparison.*"

Step4: "*Calculate the final priority weight for the factors and the sub-factors (Figure 5).*"

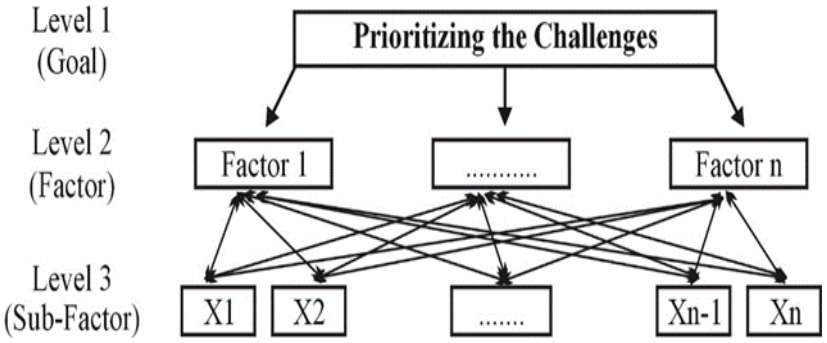

FIGURE 3. Fuzzy AHP decision hierarchy.

However, the classical AHP has several benefits, but it has some limitation due to usability of AHP in Crisp environment, judgmental scale is unbalanced, and absence of uncertainty, selection of judgment is subjective. Therefore, fuzzy AHP, a fuzzy extension of AHP, was introduced to solve more accurately for the real-time and uncertain problem [54]. The FAHP can capture the uncertain imprecise judgment of different experts by handling the linguistic variables. Various researchers have followed the Fuzzy AHP methods in a variety of domains [55]. In our study, we have utilized the fuzzy AHP developed by Chang [56], which provides more accurate and consistent results as compared to other fuzzy AHP techniques.

In a prioritization problem, let $X = \{x_1, x_2, \ldots, x_n\}$ represent the elements of main categories as an object set and $U = \{u_1, u_2, \ldots, u_n\}$ represent the elements of each category as a goal set. By Chang [56] methodology, each object is considered, and extent analysis for each goal (gi) is executed, respectively. Thus, for each object, there are (m) extent analysis values that can be obtained with the following Equation (2) and (3):

$$F_{gi}^1, F_{gi}^2, \ldots, F_{gi}^m, \tag{2}$$

$$i = 1, 2, \ldots, n \tag{3}$$

where, all $F_{gi,}^{j}$ (j = 1, 2, . . . , m) are fuzzy triangular numbers (TFNs).

The following are the key steps of Chang's extent analysis method [56]:

Step 1: The value of a fuzzy synthetic extent concerning the i^{th} object can be defined using Eq. 4:

$$S_i = \sum_{j=1}^{m} F_{gi}^j \otimes \left[\sum_{i=1}^{n}\sum_{j=1}^{m} F_{gi}^j\right]^{-1} \tag{4}$$

To achieve the expression $\sum_{j=1}^{m} F_{gi}^j$, execute the fuzzy addition operation of m extent analysis such as:

$$\sum_{j=1}^{m} F_{gi}^j = \left(\sum_{j=1}^{m} f_{gi}^l, \sum_{j=1}^{m} f_{gi}^m, \sum_{j=1}^{m} f_{gi}^u\right) \tag{5}$$

and to achieve the expression $\left[\sum_{i=1}^{n}\sum_{j=1}^{m} F_{gi}^j\right]^{-1}$, the fuzzy addition operation is executed on $F_{gi}^j (j = 1, 2, \ldots m)$ value, as follow:

$$\sum_{i=1}^{n}\sum_{j=1}^{m} F_{gi}^j = \left(\sum_{i=1}^{n} f_i^l, \sum_{i=1}^{n} f_i^m, \sum_{i=1}^{n} f_i^u\right) \tag{6}$$

and finally, calculate the inverse of the vector with the help of Eq. (7):

$$\left[\sum_{i=1}^{n}\sum_{j=1}^{m} F_{gi}^j\right]^{-1} = \left(\frac{1}{\sum_{i=1}^{n} f_i^u}, \frac{1}{\sum_{i=1}^{n} f_i^m}, \frac{1}{\sum_{i=1}^{n} f_i^l}\right) \tag{7}$$

Step 2: As F_a and F_b are two triangular fuzzy number then the degree of possibility of $F_a = (f_a^l, f_a^m, f_a^u) \geq F_b = (f_b^l, f_b^m, f_b^u)$ is defined as follows.

$$V(F_a \geq F_b) = sup[min(\mu F_a(x), (\mu F_b(x))] \tag{8}$$

The Equation 8 can be also similarly specified as below:

$$V(F_a \geq F_b) = hgt(F_a \cap F_b) = \mu_{F_a}(d) = \begin{cases} 1 & if\ f_a^m \geq f_b^m \\ \dfrac{f_a^u - f_b^l}{(f_a^u - f_a^m) + (f_b^m - f_b^l)} & f_b^l \leq f_a^u \\ 0 & Otherwise \end{cases} \tag{9}$$

Here, d represents the ordinate of the highest intersection point between D, μF_a and μ_{Fb} (Figure 4). The values of $V_1(F_a \geq F_b)$ and $V_2(F_a \geq F_b)$ are mandatory for calculating the value of P_1 and P_2.

Step 3: Calculate the overall degree of possibility of a convex fuzzy number and the other convex fuzzy numbers $F_i (i = 1, 2, \ldots, k)$ can be defined as follow:

$$V(F \geq F_1, F_2, F_3 \ldots F_k) = \min V(F \geq F_i) \tag{10}$$

Assuming that,

$$d'(F_i) = \min V(F_i \geq F_k) \tag{11}$$

for k = 1, 2, . . . , n; $k \neq i$.

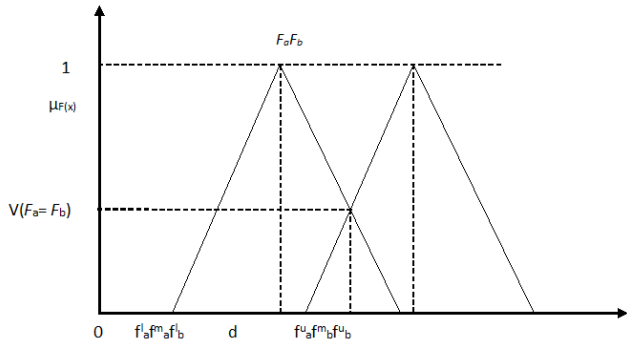

FIGURE 4. Triangular fuzzy number.

With the help of Eq. 12, calculate the weight vector using Eq. 11.

$$W' = (d'(F_1),\ d'(F_2),\ d'(F_3), \ldots d'(F_n)) \tag{12}$$

where, $F_i (i = 1, 2, \ldots, n)$ are n distinct elements.

Step 4: Via normalization, the normalized weight vectors are in equation 13, and the result will be a non-fuzzy number which represents the priority weight of the criteria:

$$W = (d(F_1),\ d(F_2),\ d(F_3), \ldots d(F_n)) \tag{13}$$

where W is a non-fuzzy number.

Step 5: Checking consistency ratio: The pairwise matrices should always be consistent in fuzzy AHP [57]. Therefore, it is necessary to check the consistency ratio of each pair-wise comparison matrices. To do so, the graded mean integration approach is utilized for defuzzifying the matrix. A triangular fuzzy number, denoted as P = (l, m, u), can be defuzzified to a crisp number as follows:

$$P_{crisp} = \frac{(4m + l + u)}{6} \tag{14}$$

After the defuzzification of each value in the matrix, consistency ratio (CR) of the matrix can easily be calculated and checked whether CR is smaller than 0.10 or not. For this, two basic parameters, i.e. Consistency Index (CI) and Consistency Ratio (CR) are used. The value of CI and CR can be calculated using Equations 14 and 15.

$$CI = \frac{\lambda_{\max} - n}{n - 1} \tag{15}$$

$$CR = \frac{CI}{RI} \tag{16}$$

where,

$\lambda_{\max}$: the largest eigenvalue of the comparison matrix,

n: the number of items being compared in the matrix and

RI: the random index and its value can be opted from Table 3.

To have a consistent matrix, the computed value of CR should less than 0.10. If the value of CR is found to be greater than 0.10, the decision-maker must again conduct the pairwise judgments."

TABLE 3. Random consistency index (RI) with respect to matrix size.

Size of the matrix	1	2	3	4	5	6	7	8	9	10
RI	0	0	0.58	0.9	1.12	1.24	1.32	1.41	1.45	1.49

IV. STUDY FINDINGS

This section contains the results and analysis of this study.

A. IDENTIFIED LIST OF CHALLENGES

By conducting the literature review, the potentiation challenging factors were identified. The identified list of challenging factors is presented in Table 4, and are briefly discussed below:

1) SMART CITY

Cities are being deployed with IoT-enabled smart devices in order to enhance i.e. vehicle to everything (V2X) connectivity, smart trash collection, crime management and other community services. These cities are integrated with information and communication technology (ICT) and various sensing devices in order to optimize the efficiency of smart city [58]. However, these devices are connected to internet that may prone to several security and privacy threats [58]. Following are the key challenges for smart city as reported in the literature.

2) BOTNET ATTACKS ON SMART CITIES

Smart city comprises of IoT-based smart devices that are more vulnerable to several security threats as these devices are designed with less security measures compared to mobile phones and computers. Thus, IoT botnet such as Mirai botnet, which targets several smart devices i.e. routers, surveillance cameras, printers, webcams causing DDoS attack in heterogenous IoT devices [59], [60]. Therefore, security experts should develop a comprehensive defense model in order to prevent such novel attacks [61].

3) DISCLOSURE OF PRIVACY

In order to achieve several objectives of smart city such as city planning, healthcare services, efficient transportation system and virtual reality, privacy plays an important role [62]. To avoid privacy leakage of sensitive information the unsecured communication between VR devices and information shared with third party, and data stored in IoT devices should be measured at each phase [63], [64].

4) AI INFLUENCE ON SMART CITY SECURITY

AI indispensable role cannot be ignored in current technological era. The rapid growth in artificial intelligence may permit attacker to build and train models in order to reveal sensitive information. For example, service providers and devices manufacturer may use machine learning and data mining models in order to extract and analyze device owner's information [65]. Though, hackers are getting intelligent in

term of understanding machine-learning algorithms used in devices. Therefore, attacker could adopt targeted approach in order to deteriorate the training effect and reliability of algorithm [66].

5) INTRUSION DETECTION

Smart city could be secured if it has capability to detect mysterious activity on time. Conventional approaches such as intrusion detection system (IDS) is used to detect three aspects i.e. specification-based detection, misuse detection, anomaly detection [67]. However, such approaches fails to meet the requirements of IoT (heterogeneous) and complex smart city network because IoT devices comprised of low battery and computation power. Thus, there need to develop a lightweight intrusion detection model and intrusion prediction system (IPS) [68] for heterogeneous network in order to predict and prevent various attacks.

6) ROUGH NODE DETECTION

Smart cities comprised of several heterogenous IoT devices in order to achieve various objectives. However, malicious IoT node could be connected to IoT system in order to collect and exchange data from other devices. Rough node could cause user's privacy leakage and could send data to neighboring node to interrupt their behavior. Ma *et al.* [69] has proposed an approach that could detect rough node in Wi-Fi based network. However, these approaches are not enough in order to achieve the smart cities security.

7) BIG DATA POSE SECURITY THREAT

Increasing number of IoT devices connected to smart city will generate huge amount of data. However, these devices do not have potential to store and process data, therefore data generated by these devices need to be sent to cloud in order to process and analyze [70]. Thus, IoT devices do not have enough capability to encrypt and decrypt data that pose the integrity and authenticity of data as critical challenge [71].

8) SMART HOME

Conventional homes have been transformed to smart homes by permitting end users to control the digital home appliances i.e. lightning, air conditioner, locks, baby monitor that are directly connected to smart phones through internet, promising to ease the human life. However, these smart devices i.e. digital appliances, locks, air conditioner connected to public and private network introduce several security and privacy attacks. Recently, hackers have compromised household devices in order to carry out spam email attacks. We have reviewed the through literature and extracted several security and privacy threats as discussed below.

9) CONFIDENTIALITY, INTEGRITY, AVAILABILITY (CIA)

IoT-enabled smart devices must ensure that personal information should be kept private from unauthorized access. Generally, cryptographic algorithms are used to ensure data privacy from unauthorized access. Due to low power and computation of IoT devices there is a risk of malicious attacks and leakage of personal information, as advanced cryptographic techniques could not be employed [72]. On the other hand, integrity ensures that information should be secured during communication and should not be accessed by unauthorized nodes. Therefore, to ensure integrity several hash functions and digital signature techniques could be used, but still these techniques are not sufficient in order to maintain integrity [73]. Furthermore, these devices send data over the network and some malicious nodes may access the information that can deteriorates the users or device availability. Thus, this forged information may trigger a fire in the device that could lead to bring financial or life lose [74].

10) SECURE-AUTO CONFIGURATION

The smart world anticipated that several smart home appliances will be interconnected to home network. However, these devices need to be configured to home network repetitively and may prone to different security attacks. This could be tedious task for householder in order to manage these devices manually so external expert need to be called to control several security threats. Therefore, there is need to implement a secure auto-configuration approach in order to achieve the smart home security [75], [76].

11) IoT SOFTWARE AND FIRMWARE UPDATES

Several mobiles and desktop operating systems are regularly updating and configuring security threats automatically. However, IoT devices consisting of software and hardware are less in numbers and due to heterogeneous nature, firmware is not updated frequently that causes a variety of security threats [77]. Thus, firmware of IoT devices for smart homes need to be updated automatically in order to cope with novel security vulnerability, as there is lack of technical support [78]. Furthermore, in order to prevent tempering and to ensure the integrity and authenticity of updates, there is a need to implement a certificate based digital signature scheme [79].

12) DoS/DDoS

Smart home network could be compromised by attacker and permit them to send RTS (Request to send)/CTS (clear to send) messages in bulk. Thus, smart devices should be capable enough to stop these devices from receiving messages in bulk and deplete their resources [80]. Several approaches have been introduced such as rate limiting [81], null0 routing [82] in order to prevent Dos/DDoS, but these are not sufficient to achieve the security of smart homes.

13) INTERDEPENDENCE BEHAVIOR OF DEVICES

Various smart home devices connected each other in a network in order to achieve a particular objective, For example if the temperature or air condition increase and reach to threshold level detected by sensor then smart plug turn on the air conditioner or open the window if it is off. Though, system itself might not be hacked by attacker but they could

change the behavior of other connected devices in order to breach physical security. This interdependence behavior of IoT smart devices is a critical challenge to achieve certain security level [83], [84].

14) TRESPASS

Several smart home devices could be compromised and permit attacker to trespass into home, which could be dangerous for life and property. For example, smart door lock could be hacked by malicious code or could accessed by unauthorized user [85]. Thus, attacker can trespass into the home without smashing door. However, various techniques could be used such as changing password frequently [86], but this could not be enough in order to achieve smart home security.

15) FALSIFICATION

Smart home devices communicate with application server in order to achieve services. Attacker could compromise the gateway routing table and could collect packets that will permit them to get confidential information [87]. However, SSL (secure socket layer) technique [88] is used, an attacker can bypass the forged certificate. Though, this technique is not enough to secure the smart home.

16) SMART HEALTHCARE

IoT devices are being developed in order to achieve smart healthcare objectives as these devices are widely used for monitoring and assessment of patient's health. Personal Medical Devices (PMD) are small sensing devices that are either planted internally or externally to patient's body in order to monitor patient's body condition. However, smart medical sensors are more prone to security threats. These devices require strong measure in order to ensure the security, privacy, integrity, confidentiality of patient's health record.

17) DEVICE HIJACKING

Smart medical IoT devices could be tampered by attackers that could be harmful for patient's health. Medical devices could also be hacked in order to steal personal information. A report revealed by TrapX [89], which interprets that most of smart medical devices are vulnerable to hijacking in different organizations i.e. blood gas analyzer and insulin pump etc. [90]. However, few researches have been conducted in order to prevent hijacking of sensors [90]. Though, there need to be developed a model in order to secure medical devices being hijacked.

18) DATA MODIFICATION

Medical devices planted internally or externally on patients' body could be intercepted by malicious nodes. However, these devices transmit data to cloud or to caregiver who could further analyze medical information in order to provide prescription, if data is altered by attackers it could be dangerous for patients' health [91]. Thus, data collected by (PMD) should be secured by attackers.

19) SECURE LOCALIZATION

Smart medical sensors support patient's movement in order to get the exact location of patient in emergency case. Location tracking system transmit location information using radio frequency, ultrasound, geo-positioning system or by some other techniques [92]. However, location could be altered by attackers if he/she could receive radio signal and analyze them, if the location information altered by attacker this could impede emergency services [93]. Thus, there is a need to develop secure location based algorithms in order to prevent location privacy.

20) TRUST MANAGEMENT

Trust is the main challenge for IoT industry while developing medical devices and sensors. In Behrouz *et al.* [94] define the trust as ''the degree to which a node should be trustworthy, secure, or reliable during any interaction with the node''. Patient could be very conscious in order to use medical devices as these devices contain their sensitive information about particular disease and could be revealed by attackers [95]. Therefore, trust management approach is needed in order to detect the degree of trust of a device.

21) FORWARD AND BACKWARD SECRECY

Smart IoT devices are evolving day by day as new invention comes into existence. Therefore, old medical devices or sensors replaced by innovative one if old one is failed to work properly. Thus, old medical device should not be able to read transmitted message if it is linked with new network [96]. It could be stolen by attackers so he/she could use for malicious purpose [97]. Similarly, new deployed device should not read the previous information [97]. A robust approach needs to address such issues.

22) SMART WEARABLE IoT

Smart devices can be worn on human body in order to monitor and analyze person's activities. These devices include smart watches, smart glasses, wristbands or jewelry items. Wearable devices are defined by six main characteristics, which are un-monopolizing, unrestrictive, observable, controllable, attentive and communicative [3]. However, these resource-constrained devices pose several security threats, which could reveal personal private information.

23) UNSECURE COMMUNICATION VIA BLUETOOTH OR ZigBee

In order to monitor and send collected data from several sensors to smart phone, smart wearable devices transmit data via short-range wireless communication technology such as Bluetooth, ZigBee [98]. However, attacker could exploit the bug in the devices to get access to locally stored data [98]. For example, attacker could use sniffers to extract unauthorized data while smart devices broadcast secret information to phone [99]. Thus, there could be a loss of secret information or life.

TABLE 4. List of identified challenges.

Sr. No	Challenges	IDs
C1	Botnet attacks on Smart Cities	[4], [13], [17]
C2	Disclosure of Privacy	[22], [33], [69], [88]
C3	AI influence on smart city security	[103],[23]
C4	Intrusion detection	[87],[67],[9],[74]
C5	Rough Node Detection	[17],[70],[91],[24]
C6	Big data pose security threat	[16],[20],[66]
C7	Confidentiality, Integrity, Availability (CIA)	[19],[4],[33][28][97]
C8	Secure-auto configuration	[22],[19],[27],[81]
C9	IoT Software and Firmware updates	[16],[29],[87],[93]
C10	DoS/DDoS	[59],[73],[82],[95]
C11	Interdependence behaviour of devices	[102],[9],[18]
C12	Trespass	[11],[69],[85]
C13	Falsification	[17],[27],[65]
C14	Device Hijacking	[87],[84],[96],[77],[90]
C15	Data Modification	[11],[22],[88]
C16	Secure Localization	[20],[15],[77],[19]
C17	Trust Management	[6],[8],[64]
C18	Forward and backward secrecy	[2],[70],[72],[74][88]
C19	Unsecure communication via Bluetooth or ZigBee	[6],[17],[26]
C20	Stolen device may compromise security	[78],[83],[93]
C21	Lack of authentication and authorization	[65],[69],[79],[89]

24) STOLEN DEVICE MAY COMPROMISE SECURITY

Wearable IoT devices carrying personal secret information could be stolen or lost. The stolen or lost smart devices could compromise the confidentiality, integrity and availability if it has fallen into attacker's hand [100]. These smart devices come without any built-in security mechanism and store data without any encryption [100]. Thus, personal data and secret information could be revealed.

25) LACK OF AUTHENTICATION AND AUTHORIZATION

Smart devices come without any built-in security mechanism and these devices store data locally without any encryption method [101]. Beside this, there need to ensure data integrity, confidently and other security services as HP study [102] revealed that 30 percent of smart watches are vulnerable of security issues. Furthermore, strong cryptographic algorithm could not be implemented because these devices are resource constrained [103]. The list of investigated challenging factors are enlisted in Table 4.

As the aim of this study is to develop a prioritization based taxonomy of the identified IoT challenging factors. Though, to develop the hierarchy structure of the research problem of this study, we mapped the identified list of challenges into core domain of IoT i.e. ''smart home'', ''smart city'', ''smart healthcare'' and ''IoT wearable's''. All the authors of this study participated and classified the identified list of challenges in the core domains of IoT using the coding scheme [104]. All the steps of coding scheme i.e., ''code,'' ''sub-categories,'' ''categories'' and ''theory'' were carefully performed. The mapped challenging factors against each knowledge area is given in Figure 5.

B. RESULTS OF EMPIRICAL STUDY

The main objective of this empirical study is to get opinions of industrial experts in terms to get their insight regarding the identified challenge and their core categories. The collected responses were summarized into three core categorize that include positive ''agree, and strongly agree'', negative (disagree and strongly disagree) and neutral. The responses of positive category refers to the survey respondents who are agree with as the identified challenges have negative influence on IoT paradigm. The results of negative category shows that the identified challenges do not have negative influence on IoT paradigm. Moreover, the neutral category shows that participants are not sure about the effect of identified challenge on IoT. The summarized detail of survey respondents is given in Table 5.

The responses of survey participants are analyzed using the frequency analysis approach and the summarized results are presented in Table 5. The results shows that C7 (Confidentiality, Integrity, Availability (CIA), 94%) is declared as the highest scored challenging factor for secure IoT. IoT-enabled smart devices must ensure that personal information should be kept private from unauthorized access. Generally, cryptographic algorithms are used to ensure data privacy from unauthorized access. Due to low power and computation of IoT devices there is a risk of malicious attacks and leakage of personal information, as advanced cryptographic techniques could not be employed [73]. On the other

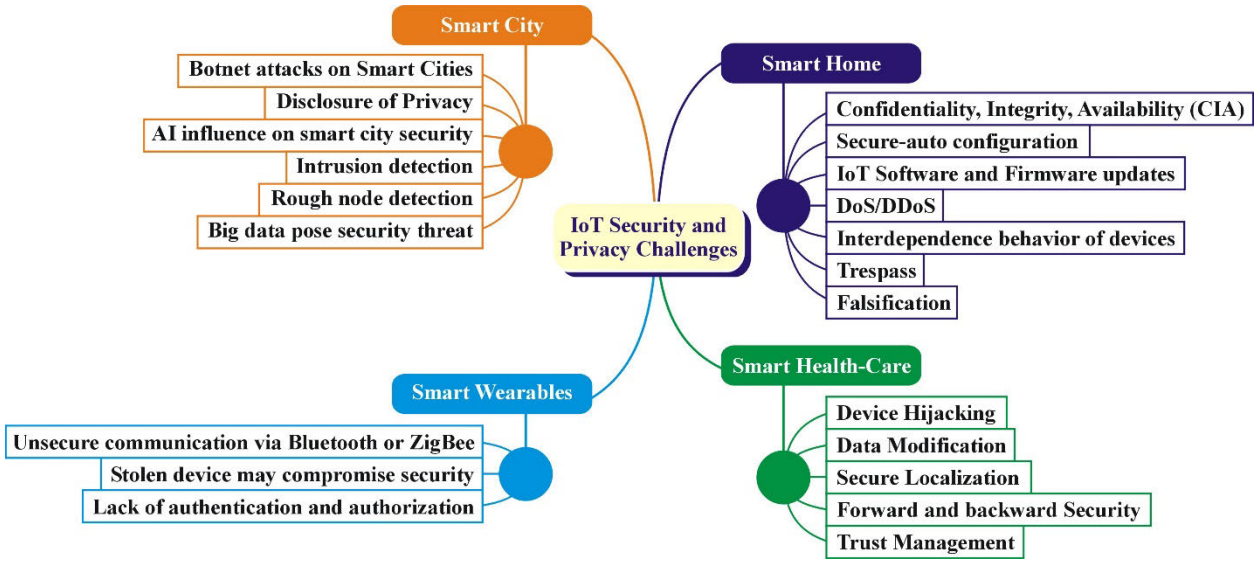

FIGURE 5. Mapping of identified challenges into core domains.

TABLE 5. Empirical investigation.

S.NO	List of challenges	Number of Responses (N=50)							
		Positive			Negative			Neutral	
		S. A	A	%	D	S.D	%	N	%
P1	**Smart City**	**24**	**21**	**90**	**3**	**0**	**6**	**2**	**4**
C1	Botnet attacks on Smart Cities	30	15	90	2	1	6	2	4
C2	Disclosure of Privacy	16	24	80	4	2	12	4	8
C3	AI influence on smart city security	19	18	74	7	3	20	3	6
C4	Intrusion detection	21	18	78	3	3	12	5	10
C5	Rough Node Detection	14	19	66	6	3	18	8	16
C6	Big data pose security threat	9	15	48	12	5	17	9	18
P2	**Smart Homes**	**21**	**14**	**70**	**5**	**3**	**16**	**7**	**14**
C7	Confidentiality, Integrity, Availability (CIA)	35	12	94	0	0	0	3	6
C8	Secure-auto configuration	17	14	62	5	7	24	7	14
C9	IoT Software and Firmware updates	13	16	58	9	3	24	9	18
C10	DoS/DDoS	21	16	74	5	3	16	5	10
C11	Interdependence behavior of devices	13	12	50	10	8	36	7	14
C12	Trespass	16	15	62	4	6	10	9	18
C13	Falsification	18	15	66	8	3	22	6	12
P3	**Smart Healthcare**	**22**	**16**	**76**	**3**	**4**	**14**	**5**	**10**
C14	Device Hijacking	18	16	68	5	3	16	8	16
C15	Data Modification	16	15	62	4	6	10	9	18
C16	Secure Localization	21	15	72	4	3	14	7	14
C17	Trust Management	22	17	78	3	2	10	6	12
C18	Forward and backward secrecy	17	15	64	3	3	12	12	24
P4	**Smart Wearables**	**22**	**13**	**70**	**4**	**5**	**18**	**6**	**12**
C19	Unsecure communication via Bluetooth or ZigBee	18	15	66	8	3	22	6	12
C20	Stolen device may compromise security	15	12	54	3	5	16	15	30
C21	Lack of authentication and authorization	22	13	70	3	5	16	7	14

hand, integrity ensures that information should be secured during communication and should not be accessed by unauthorized nodes [74]. We further noted that C1 (Botnet attacks on Smart Cities, 90%) and C2 (Disclosure of Privacy, 80%) are declared as the second and third most important challenges for secure IoT.

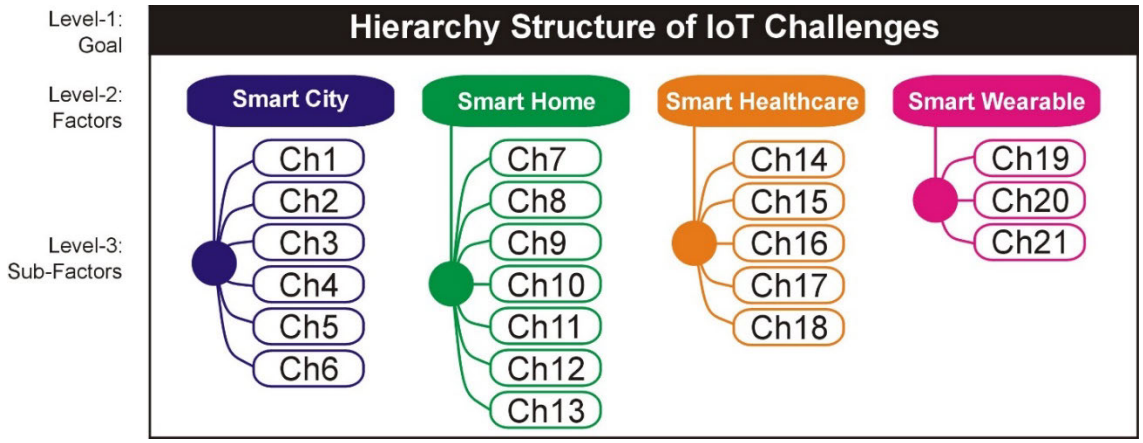

FIGURE 6. Proposed hierarchy structure.

The results of negative category renders that C11 (Interdependence behavior of devices, 36%) is declared as the highest reported challenging factor in negative category. This indicated that 36% of the survey participants are not agree with the negative impact of C11. We also noted that C8 (Secure-auto configuration, 24%) and C9 (IoT Software and Firmware updates, 24%) are declared as the 2nd highest reported challenges in negative category.

Moreover, the responses against each category of IoT challenges indicated that P1 (Smart City, 90%), P3 (Smart Healthcare, 76%), P2 (Smart Homes, 70%) and P4 (Smart Wearables, 70%) are ranked as the first, second and third highest ranked categories of IoT challenges.

C. APPLICATION OF FUZZY ANALYTICAL HIERARCHY PROCESS (FAHP) FOR PRIORITIZING THE COSD CHALLENGES

To determine the priorities of identified challenges and their categories, we applied the fuzzy-AHP approach. All the adopted steps of fuzzy-AHP are performed in the sub-sequent sections:

Step-1 (Proposed Hierarchy Structure of Identified Challenges and Their Categories): In order to perform the fuzzy-AHP, firstly, we have develop a hierarchy structure of the challenges by following the Figure 3. The hierarchy structure is based on the mapping of identified challenges in the core areas of IoT (section3.3). The key objective of the study problem is mentioned on top level and the sub-categories and their respective challenges are presented on level-2 and level-3, respectively (Figure 6). The developed hierarchy helps to perform the fuzzy-AHP analysis which is presented in the following steps.

Step-2 (Conducting the Pairwise Comparison): The purpose "of this study is to prioritize the identified challenging factors and their categories concerning their significance for the secure IoT. To perform the pairwise comparison (for fuzzy-AHP analysis), we have developed a questionnaire and contacted respondents of the first survey. A total of 28 responses were received from the survey participants. All the responses were manually reviewed to check for incomplete data. We found that all the 28 responses were complete. A sample of the pairwise questionnaire survey (second survey) is given in Appendix-B. Small sample size can be one potential issue with application of fuzzy-AHP analysis. However, a number of existing studies have used similar dataset to perform the AHP analysis [105]–[108]. For example, Shameem *et al.* [109] conducted an AHP analysis to prioritize the influencing factors of distributed agile software development based on the responses collected from five experts. Similarly, Cheng and Li [107] prioritize the success factors of construction partnering by considering the data collected from nine experts. Lam and Zhao [108] conducted a survey study with eight experts to investigate the influencing factors of teaching quality. Moreover, Cheng and Li [107] conducted an AHP analysis for the selection of intelligent buildings system by considering the responses collected from nine experts. Therefore, we have performed FAHP analysis by considering the data collected from 31 experts which is acceptable sample size for generalizing the results of this study."

The data collected via the "fuzzy-AHP survey were transformed in geometric mean to evaluate the pairwise comparison of the COSD challenges and their respective categories. The geometric mean is useful to transform the expert's judgments into TFN numbers; the formula used to apply the geometric mean is given below:"

$$\begin{aligned} \text{Geometric mean} &= \sqrt[n]{a1x\ a2 \times a3 \ldots\ldots\ldots an} \\ a &= \text{Weight of each response} \\ n &= \text{Number of responses} \end{aligned} \tag{17}$$

Linguistic variable against their triangular fuzzy Likert scales is given in Table 6. To develop the pairwise comparison matrixes of the investigated challenges and their categories; the triangular fuzzy conversion scale (Table 6), proposed by Bozbura *et al.* [110] was adopted."

TABLE 6. Triangular fuzzy conversion scale [110].

Linguistic Scale	Triangular Fuzzy scale	Triangular Fuzzy Reciprocal scale
Just equal (JE)	(1,1,1)	(1,1,1)
Equally important (EI)	(1/2,1,3/2)	(2/3,1,2)
Weakly important (WI)	(1,3/2,2)	(1/2,2/3,1)
Strong more important (SMI)	(3/2,2,5/2)	(2/5,1/2,2/3)
Very strong more important (VSMI)	(2,5/2,3)	(1/3,2/5,1/2)
Absolutely more important (AMI)	(5/2,3,7/2)	(2/7,1/3,2/5)

TABLE 7. Pairwise comparison of challenging factors categories.

Categories of the factors				
	Smart City	Smart Homes	Smart Healthcare	Smart Wearables
Smart City	(1,1,1)	(1.5, 2.5, 3)	(1, 1.5, 2)	(1.5, 2, 2.5)
Smart Homes	(0.3, 0.4, 0.6)	(1,1,1)	(0.4, 0.5, 0.6)	(0.5, 0.6. 1)
Smart Healthcare	(0.5, 0.6, 1)	(1.5, 2, 2.5)	(1,1,1)	(1, 1.5, 2)
Smart Wearables	(0.4, 0.5, 0.6)	(1, 1.5, 2)	(0.5, 0.6. 1)	(1,1,1)

Step-3 (Calculating the Local Priority Weight of Each Success Factor and Their Respective Categories: A Numerical Example): The priority vector of each main category of challenges is listed in Table 7. Local Priority Weight (LPW) of all the main categories of the factors were calculated using Equation 3. First, the synthetic extent values of four categories, i.e. Organizational Management, process, technology, and coordination in were determined, and the priority weight of each category was calculated using Equation 4. We have provided the calculation of priority weight for all the categories of the challenges as, $\sum_{i}^{n}\sum_{j}^{m} F_{gi}^{j}, \left[\sum_{i}^{n}\sum_{j}^{m} F_{gi}^{j}\right]^{-1}$, $\sum_{j=1}^{m} F_{g1}^{j}$, $\sum_{j=1}^{m} F_{g2}^{j}$, $\sum_{j=1}^{m} F_{g3}^{j}$, and $\sum_{j=1}^{m} F_{g4}^{j}$, as shown at the bottom of the next page.

"The ""Smart City (SC), "Smart Homes" (SH), "Smart Healthcare" (SHC), and "Smart Wearables" (SW) represent the synthesis values of main categories which were calculated using Equation 4 as follow:

$$\begin{aligned} SC &= \sum_{j}^{m} F_{g1}^{j} \otimes \left[\sum_{i}^{n}\sum_{j}^{m} F_{gi}^{j}\right]^{-1} \\ &= (5, 7, 8.5) \otimes (0.04386, 0.054945, 0.070922) \\ &= (0.219298, 0.384615, 0.602837) \\ SH &= (2.2, 2.5, 3.2) \otimes (0.04386, 0.054945, 0.070922) \\ &= (0.096491, 0.137363, 0.226950) \\ SHC &= (4, 5.1, 6.5) \otimes (0.04386, 0.054945, 0.070922) \\ &= (0.175439, 0.280220, 0.460993) \\ SW &= (2.9, 3.6, 4.6) \otimes (0.04386, 0.054945, 0.070922) \\ &= (0.127193, 0.197802, 0.326241) \end{aligned}$$

The degree of possibility using Equation 6 is determined. The minimum degree of possibility (priority weight) for each pair-wise comparison was calculated using Equation 8.

TABLE 8. Results of V values for criteria.

	SC	SH	SHC	SW	d (Priority Weight)
V(SC≥….)	-	1	1	1	1
V(SH≥….)	0.030019	-	0.26502	0.62272	0.030019
V (SHC ≥)	0.69836	1	-	1	0.69836
V (SW ≥)	0.36405	1	0.64661	-	0.36405

Therefore, "the weight vector was determined as $W' = (1, 0.030019, 0.69836, 0.36405)$ (Table 8). When these values were normalized, the importance of attributes were calculated as $W = (0.4789, 0.01435, 0.3337)$. The given results reveal that organizational management is the most significant category as it has highest priority weight as compared to the other categories of the challenge factors."

Step-4 (Test the Consistency of the Pair-Wise Matrix): In this section, "we presented a step-by-step calculation of the procedure followed to check whether a given pairwise matrix is consistent or not. For this, we have considered the Table of Categories (Table 9). A triangular fuzzy number of the pair-wise comparison matrix of the main categories are defuzzified to crisp number using Equation 14 and obtained the corresponding Fuzzy Crisp Matrix (FCM) as shown in Table 9:"

The largest Eigen vector (λ_{max}) "value of the FCM matrix is calculated by calculating the column sum of each column of FCM matrix (Table 9) and then divide each element of FCM matrix by column sum. Moreover, the priority weight is calculated by taking the average of each row, as shown in Table 10."

$$\lambda_{max} = \sum([\sum Cj] \times \{W\} \tag{18}$$

where, $\sum Cj$ = sum of the columns of Matrix [C] (Table 7),

W = weight vector (Table 10), therefore

$\lambda_{max} = 2.7{*}0.37938 + 7.0{*}0.14945 + 3.7{*}0.27593 + 5.2{*}0.19524 = 4.1067$

TABLE 9. Fuzzy Crisp Matrix (FCM) for challenge factors categories.

	Smart City	Smart Homes	Smart Healthcare	Smart Wearables
Smart City	1.0	2.5	1.5	2.0
Smart Homes	0.5	1.0	0.5	0.7
Smart Healthcare	0.7	2.0	1.0	1.5
Smart Wearables	0.5	1.5	0.7	1.0
Column Sum	2.7	7.0	3.7	5.2

Based on "the calculation, the largest Eigen value (λmax) of the matrix FCM is 4.1067. The dimension of FCM is 4. Therefore n = 4 and the Random Consistency Index (RI) is 0.9 for n = 4 (Table 3). Therefore, equation 15 and 16 are used to calculate the consistency index and consistency ration as follows:

$$CI = \frac{\lambda_{\max} - n}{n-1} = \frac{4.1067 - 4}{4-1} = 0.035553$$
$$CR = \frac{CI}{RI} = \frac{0.035553}{0.9} = 0.039503$$

The calculated value of CR is 0.039503<0.10; therefore, the pairwise comparison matrix developed for the categories of success factors is consistent and acceptable. Similarly, the consistency ratio for all the categories are checked, and the results along with pairwise comparison are given in Table 11 to 14."

Phase 5 Determining the Ranking of the Success Factors: The summarized weights and their corresponding rankings are given in Table15. The local rank (LR) of each challenging factor was calculated considering the determined weight of each challenge within their respective category. For example, the first category (smart city) contains six challenges and out of them C3 (AI influence on smart city security, LW = 0.420) is standout as the highest priority challenge for IoT paradigm. We further noted that C1 (Botnet attacks on Smart Cities, LW = 0.378) and C5 (Rough Node Detection, LW = 0.201) are standout second and third most significant challenging factors within *Smart City* category, respectively. By using the same method the local ranks of each challenging factors and their corresponding categories were determined (Table 15). The local ranks indicates the priority order of a challenging factor within their respective categories. The local ranking server as a knowledge base for real-world experts to consider the highest ranked challenges with respect to their job designation and interest.

Moreover, to get the impact of each identified challenge on overall IoT paradigm, we determined the global weight (GW). Using the GW, the global ranks for each challenging factor was determined. The global rank was determined by multiplying the local weigh of a factors with its category weight. For example, the GW of C1 = LW of C1 × category weigh (i.e. Smart City); GW of C1 = 0.378 × 0.37938 = GW = 0.1434. Based on the rankings of all the challenging factors it is found that C1 is standout at the 2nd most priority challenging factor compared with all the other 20 challenges. Likewise, the global ranks for each challenging factor was determined and the results are given in Table 15. The results shows that C3 (AI influence on smart city security, GW = 0.1593) is declared as the top ranked challenging factor for the secure IoT. The results shows that C15 (Data modification GW = 0.0943) and C18 (Forward and backward secrecy, GW = 0.0881) are declared as the third and fourth most priority challenge factor for secure IoT.

Phase 6 Prioritization-Based Taxonomy of Challenges: The prioritization based taxonomy of the identified challenging factors was developed using their core categories

$$\sum_{i}^{n}\sum_{j}^{m} F_{gi}^{j} = (1,1,1) + (1.5,2,2.5) + (1,1.5,2) \ldots + (0.5,0.6,1) + (1,1,1) = (14.1, 18.2, 22.8)$$

$$\left[\sum_{i}^{n}\sum_{j}^{m} F_{gi}^{j}\right]^{-1} = \left(\frac{1}{22.8}, \frac{1}{18.2}, \frac{1}{14.1}\right) = (0.04386, 0.054945, 0.070922)$$

$$\sum_{j=1}^{m} F_{g1}^{j} = (1,1,1) + (1.5,2.5,3) + (1,1.5,2) + (1.5,2.0,2.5) = (5,7,8.5)$$

$$\sum_{j=1}^{m} F_{g2}^{j} = (0.3,0.4,0.6) + (1,1,1) + (0.4,0.5,0.6) + (0.5,0.6,1) = (2.2,2.5,3.2)$$

$$\sum_{j=1}^{m} F_{g3}^{j} = (0.5,0.6,1) + (1.5,2,2.5) + (1,1,1) + (1,1.5,2) = (4,5.1,6.5)$$

$$\sum_{j=1}^{m} F_{g4}^{j} = (0.4,0.5,0.6) + (1,1.5,2) + (0.5,0.6,1) + (1,1,1) = (2.9,3.6,4.6)$$

TABLE 10. Normalized matrix of challenge factors categories.

	Smart City	Smart Homes	Smart Healthcare	Smart Wearables	Priority vector weight
Smart City	0.37037	0.35714	0.40541	0.38462	0.37938
Smart Homes	0.18519	0.14286	0.13514	0.13462	0.14945
Smart Healthcare	0.25926	0.28571	0.27027	0.28846	0.27593
Smart Wearables	0.18519	0.21429	0.18919	0.19231	0.19524

TABLE 11. Pairwise comparison of smart city category challenges.

	C1	C2	C3	C4	C5	C6
C1	(1,1,1)	(1, 1.5, 2)	(2.5, 3, 3.5)	(0.6, 1, 2)	(1.5, 2, 2.5)	(1, 1.5, 2)
C2	(0.5, 0.6, 1)	(1,1,1)	(0.5, 0.6, 1)	(1, 1.5, 2)	(0.4, 0.5, 0.6)	(1, 1.5, 2)
C3	(0.2, 0.3, 0.4)	(1, 1.5, 2)	(1,1,1)	(0.5, 1, 1.5)	(0.5, 0.6, 1)	(0.5, 0.6, 1)
C4	(0.5, 1, 1.5)	(0.5, 0.6, 1)	(0.6, 1, 2)	(1,1,1)	(0.2, 0.3, 0.4)	(2, 2.5, 3)
C5	(0.4, 0.5, 0.6)	(1.5, 2, 2.5)	(1, 1.5, 2)	(2.5, 3, 3.5)	(1,1,1)	(0.4, 0.5, 0.6)
C6	(0.5, 0.6, 1)	(0.5, 0.6, 1)	(1, 1.5, 2)	(0.3, 0.4, 0.5)	(1.5, 2, 2.5)	(1,1,1)

λmax= 6.57; CI = 0.057; CR = 0.09<0.10(consistency OK)

TABLE 12. Pairwise comparison of Smart Home category challenges.

	C7	C8	C9	C10	C11	C12	C13
C7	(1,1, 1)	(1.5,2,2.5)	(1.5,2,2.5)	(0.66,1,1.5)	(1.5,2,2.5)	(1.5,2,2.5)	(1, 1.5, 2)
C8	(0.4,0.5,0.67)	(1,1, 1)	(1.5,2,2.5)	(0.66,1,1.5)	(0.66,1,1.5)	(2.5, 3, 3.5)	(0.3, 0.4, 0.5)
C9	(0.4,0.5,0.67)	(0.4,0.5,0.67)	(1,1, 1)	(0.66,1,1.5)	(0.66,1,1.5)	(0.5, 0.6, 1)	(1.5, 2, 2.5)
C10	(0.66,1,1.5)	(0.66,1,1.5)	(0.66,1,1.5)	(1,1, 1)	(0.66,1,1.5)	(1.5, 2, 2.5)	(0.4, 0.5, 0.6)
C11	(0.4,0.5,0.67)	(0.66,1,1.5)	(0.66,1,1.5)	(0.66,1,1.5)	(1,1, 1)	(0.6, 1, 2)	(2.5, 3, 3.5)
C12	(0.4,0.5,0.67)	(0.5, 0.6, 1)	(0.2, 0.3, 0.4)	(1, 1.5, 2)	(1.5, 2, 2.5)	(1,1,1)	(1, 1.5, 2)
C13	(0.5, 0.6, 1)	(2, 2.5, 3)	(0.2, 0.3, 0.4)	(0.6, 1, 2)	(0.5, 1, 1.5)	(0.5, 0.6, 1)	(1,1,1)

λmax=7.059, CI =0.066, RI =1.32, CR = 0.047<0.1 (consistency OK)

TABLE 13. Pairwise comparison of Smart healthcare category challenges.

	C14	C15	C16	C17	C18
C14	(1,1,1)	(0.3, 0.4, 0.5)	(1.5, 2, 2.5)	(0.4, 0.5, 0.6)	(0.4, 0.5, 0.6)
C15	(2, 0.5, 3)	(1,1,1)	(2, 0.5, 3)	(0.5, 1, 1.5)	(1, 1.5, 2)
C16	(0.4, 0.5, 0.6)	(0.3, 0.4, 0.5)	(1,1,1)	(2, 0.5, 3)	(2.5, 3, 3.5)
C17	(1.5, 2, 2.5)	(0.6, 1, 2)	(0.3, 0.4, 0.5)	(1,1,1)	(0.5, 0.6, 1)
C18	(1.5, 2, 2.5)	(0.5, 0.6, 1)	(0.2, 0.3, 0.4)	(1, 1.5, 2)	(1,1,1)

λmax = 5.2878; CI = 0.071950; CR = 0.064<0.10(consistency OK)

TABLE 14. Pairwise comparison of Smart Wearables category challenges.

	C19	C20	C21
C19	(1,1,1)	(1.5, 2.5, 3)	(1, 1.5, 2)
C20	(0.3, 0.4, 0.6)	(1,1,1)	(0.4, 0.5, 0.6)
C21	(0.5, 0.6, 1)	(1.5, 2, 2.5)	(1,1,1)

λmax = 3.0707; CI = 0.035553; CR = 0.061<0.10 (consistency OK)

and the determined ranks (Figure 7). The developed taxonomy present the impact of each particular challenge within their category and globally (compared with all the identified challenges). For example, C3 (AI influence on smart city security), C1 (Botnet attacks on Smart Cities) and C15 (Data Modification) are declared as the 1st, 2nd and 3rd most priority challenges. We noticed that C3 (AI influence on smart city security) and C1 (Botnet attacks on Smart Cities) are belongs to 'Smart City' category and their local ranks also stand similar with global ranks; but, C15 (Data Modification) belongs to 'Smart Healthcare' and it is stand as 1st with respect to local ranking and 3rd in global ranking. Similarly, C18 (Forward and backward secrecy) declared as 2nd ranked in with respect to local ranking and 4th by considering the

TABLE 15. Success factors ranking.

Categories	Categories Weight (CW)	Challenging Factors	Local Weights (LW)	Local Ranking (LR)	Global Weights (GW)	Global Ranking (GR)
Smart City	0.37938	C1	0.378	2	0.1434	2
		C2	0.063	6	0.0239	20
		C3	0.420	1	0.1593	1
		C4	0.180	4	0.0682	8
		C5	0.201	3	0.0762	6
		C6	0.104	5	0.0394	12
Smart Home	0.14945	C7	0.176	6	0.0263	18
		C8	0.210	4	0.0313	16
		C9	0.241	3	0.0360	14
		C10	0.191	5	0.0285	17
		C11	0.161	7	0.0240	19
		C12	0.340	2	0.0508	9
		C13	0.487	1	0.0727	7
Smart Healthcare	0.27593	C14	0.160	4	0.0441	11
		C15	0.342	1	0.0943	3
		C16	0.120	5	0.0331	15
		C17	0.182	3	0.0502	10
		C18	0.320	2	0.0881	4
Smart Wearables	0.19524	C19	0.170	3	0.0331	15
		C20	0.198	2	0.0386	13
		C21	0.430	1	0.0878	5

global ranking. The prioritization based taxonomy presents the impact of each enlisted challenge with respect their impact within the category and fore overall study objective. We believe that the developed prioritization based taxonomy will help to both academic researchers and industry experts to consider the most important set of challenges and their categories for the progression of secure IoT paradigm.

V. DISCUSSION AND SUMMARY

The basic objective of this study is to explore, classify and to prioritize the factors that could negatively impact the security and privacy in IoT paradigm. The objective of this study is meet in three different steps, firstly, the literature review study was performed to explore the challenging factor, reported by the researchers. Secondly, the findings of the literature study was further verified with experts via questionnaire survey study. Finally, the identified challenges were prioritized by applying the fuzzy-AHP approach. To address the objective of this study, three research questions has been developed, and the summary is presenting below:

A. RQ1 (What ARE THE IMPORTANT CHALLENGING FACTORS TOWARDS THE SECURE IoT PARADIGM REPORTED IN THE LITERATURE AND REAL-WORLD PRACTICES?)

In first phase of this study, we have performed the literature review and explore the factors that could hinder the security and privacy of IoT. During literature review, we have identified a list of 21 challenges that are critical for the for IoT paradigm. As the ultimate aim of this study is to develop a prioritization based taxonomy of the IoT challenging factors. Though, the identified challenges were further mapped in the core domain of IoT i.e. smart city, smart home, smart healthcare and smart wearable's. The key objective of mapping the investigated challenges into core domain of IoT is to develop a hierarchy structure in which the main objective of the study is presented on level-1, the alternative (core domains) and sub-alternatives (challenges) are presented at level-2 and 3, respectively.

In order to verify the identified challenges and their mapping process, we further conducted the questionnaire survey study with experts. During questionnaire survey study, a total of 50 complete response were collected. The collected responses were analyzed using the frequency analysis method and the results indicated that the enlisted IoT challenging factors and their categories are related to the real-world industry practices.

B. RQ2: (What WOULD BE THE PRIORITIZATION BASED TAXONOMY OF THE INVESTIGATED CHALLENGING FACTORS?)

The final step of this study is to perform the fuzzy-AHP process aiming to prioritize the investigated challenging factors and their respective core categories with respect to their

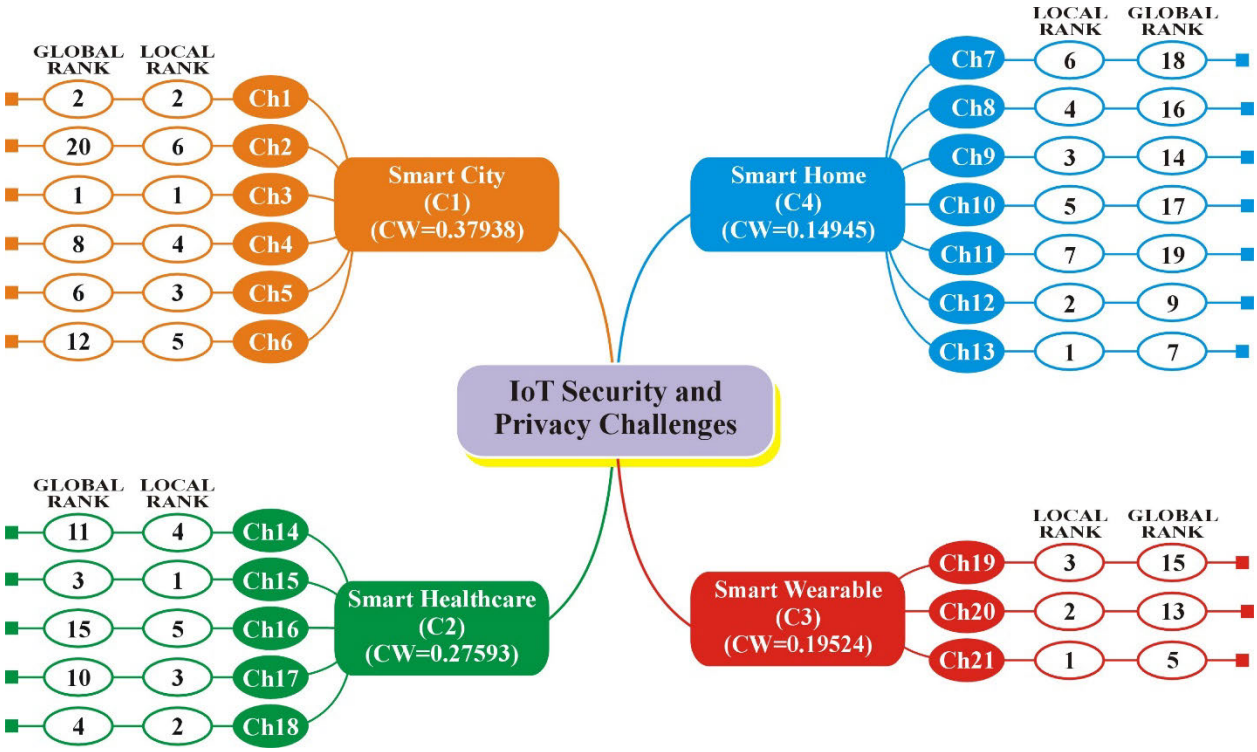

FIGURE 7. Prioritization based taxonomy of the identified challenges.

criticality to IoT security and privacy. To perform the fuzzy-AHP, we have performed the pairwise comparison approach with the experts aiming to get their opinions regarding identified challenges. By carefully applying all the steps of fuzzy-AHP, we have calculated the priority ranks of each challenging factor.

For example, C3 (AI influence on smart city security), C1 (Botnet attacks on Smart Cities) and C15 (Data Modification) are declared as the 1st, 2nd and 3rd most priority challenges. We noticed that C3 (AI influence on smart city security) and C1 (Botnet attacks on Smart Cities) are belongs to 'Smart City' category and their local ranks also stand similar with global ranks; but, C15 (Data Modification) belongs to 'Smart Healthcare' and it is stand as 1st with respect to local ranking and 3rd in global ranking. Similarly, C18 (Forward and backward secrecy) declared as 2nd ranked in with respect to local ranking and 4th by considering the global ranking. The prioritization based taxonomy presents the impact of each enlisted challenge with respect their impact within the category and fore overall study objective.''

VI. THREATS TO VALIDITY

The literature survey data ''were collected using the informal review approach and there is chance of missing some relevant data because of not formally conducting the review process. It might be threat to the internal validity of the study findings. We tried to eliminate this threat by following the snowballing data sampling approach in order to identify the most related published studies for the literature survey. Moreover, the same data collection approach has been adopted in different other research studies to identify and classify the factors [109], [111]. The empirical data were collected from 50 survey participants because of lack of resources, time and physical approach to the targeted population. The given data sample might be small to validate the identified challenging factors and their conceptual mapping. However, we consider the data samples of different other published software engineering studies, where the data were collected from 54 [112], 81 [113] and 35 [114] survey respondents. Construct validity refers to know the extent at which the survey study measures the targeted variables based on the survey scale. In this study, the survey questionnaire was developed based on the identified challenges (variables) and it was evaluated by collecting and analyzing the data from the experts. The survey results revealed that most of the respondents were agree to consider the identified challenges are critical for the security and privacy of IoT. There is possible threat of statistical conclusion validity, because the content of the survey questionnaire has been developed by the authors based on the literature findings. However, the pilot evaluation study was conducted with the software engineering experts in order to ensure the structure of the survey instrument, sampling procedure and survey assessment scale.''

VII. STUDY IMPLICATION

The findings of the study provides the state-of-the-art and state-of-the practices factors that could influence the IoT paradigm concerning to security and privacy. The literature review study was conducted to explore the list of challenges that could hinders the security and privacy of IoT paradigm;

and the questionnaire survey study present the impact of identified challenges and their core categories. The investigated list of challenging factors serve as a body of knowledge for academic researchers and industry experts with respect to the factor hinder the security and privacy of IoT paradigm.

Moreover, using the fuzzy-AHP approach, the identified list of challenges and their core categories are ranked with respect to their criticality for the security and privacy of IoT paradigm. The study provides a prioritization based taxonomy considering the challenges, their core categories and local and global ranks. The developed taxonomy serve as a framework for industry experts to focus on the most critical areas for secure IOT.

VIII. CONCLUSION AND FUTURE DIRECTIONS

Currently, the Internet of things (IoT) is an increasingly adopting phenomena. IoT providing the ways to ease the human life by sharing data in seamless manner. The current available smart devices are promising level of comfort, efficiency, and automation for users. Thus, present is witnessed the vast use of smart devices in cities, industries, agriculture and healthcare sectors. However, Smart resource facing the critical problem and the security and privacy is one of them.

Considering the significance of security and privacy parameters in IoT, we are motivated to explore and analyses the factors that could have negative impact on security and privacy of IoT. Therefore, via literature review, a total of 21 challenging factors has been identified. The identified list of challenges were further classified in the core domain of IoT that include i.e. smart city, smart home, smart wearable's and smart health care. Moreover, the questionnaire survey study was conducted with the experts aiming to get the perceptions of experts concerning to the identified list of challenges form literature review and their mapping in core categories of IoT. The questionnaire survey results shows that the identified list of challenges and their categories are related with real-world practices.

Furthermore, the fuzzy-AHP approach has been applied to fix the multicriteria decision making problems. Based on the expert's opinions in pairwise comparisons, all the steps of fuzzy-AHP has been applied and local and global ranks for each challenging factors was determined. The results indicated that C3 (AI influence on smart city security), C1 (Botnet attacks on Smart Cities), C15 (Data Modification), C18 (Forward and backward secrecy) and C21 (Lack of authentication and authorization) are declared as the top five ranked challenging factors for secure IoT. Using the list of identified challenges, their mapping in core IoT domains and the fuzzy-AHP analysis; this study contributed by providing a prioritization based taxonomy that will assists the practitioners and researchers to consider the high impact challenging factors concerning to the secure IoT.

In future, we will expand this study by conducting the multivocal literature review and will identify the success factors and additional challenges of secure IoT. In addition, we will conduct case studies with experts to collect the best practices for secure IoT. Based on the empirical findings, we will develop the guidelines that will assists the industry experts for the progression of secure IoT paradigm.

APPENDIXES

Sample of Used Survey Instrument: https://tinyurl.com/3cck9ypf

Sample of pairwise comparison questionnaire: https://tinyurl.com/3y6ewcxa

ACKNOWLEDGMENT

The authors are grateful to the Deanship of Scientific Research, King Saud University for funding through Vice Deanship of Scientific Research Chairs.

REFERENCES

[1] K. K. Patel and S. M. Patel, "Internet of Things-IOT: Definition, characteristics, architecture, enabling technologies, application & future challenges," *Int. J. Eng. Sci. Comput.*, vol. 6, pp. 6122–6131, 2016.
[2] S. D. T. Kelly, N. K. Suryadevara, and S. C. Mukhopadhyay, "Towards the implementation of IoT for environmental condition monitoring in homes," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3846–3853, Oct. 2013.
[3] N. Khalid, N. A. Abbasi, and O. B. Akan, "Statistical characterization and analysis of low-THz communication channel for 5G Internet of Things," *Nano Commun. Netw.*, vol. 22, Dec. 2019, Art. no. 100258.
[4] M. Bazzani, D. Conzon, A. Scalera, M. A. Spirito, and C. I. Trainito, "Enabling the IoT paradigm in e-health solutions through the VIRTUS middleware," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 1954–1959.
[5] M. S. Hossain, G. Muhammad, and A. Alamri, "Smart healthcare monitoring: A voice pathology detection paradigm for smart cities," *Multimedia Syst.*, vol. 25, no. 5, pp. 565–575, 2019.
[6] T. Lennvall, M. Gidlund, and J. Åkerberg, "Challenges when bringing IoT into industrial automation," in *Proc. IEEE AFRICON*, Sep. 2017, pp. 905–910.
[7] S. A. I. Quadri and P. Sathish, "IoT based home automation and surveillance system," in *Proc. Int. Conf. Intell. Comput. Control Syst. (ICICCS)*, Jun. 2017, pp. 861–866.
[8] C. Qiu, F. Wu, C. Lee, and M. R. Yuce, "Self-powered control interface based on gray code with hybrid triboelectric and photovoltaics energy harvesting for IoT smart home and access control applications," *Nano Energy*, vol. 70, Apr. 2020, Art. no. 104456.
[9] H. F. Atlam and G. B. Wills, "IoT security, privacy, safety and ethics," in *Digital Twin Technologies and Smart Cities*. U.K.: Springer, 2020, pp. 123–149.
[10] P. M. Chanal and M. S. Kakkasageri, "Security and privacy in IoT: A survey," *Wireless Pers. Commun.*, vol. 115, pp. 1667–1693, Jul. 2020.
[11] D. K. Alferidah and N. Jhanjhi, "A review on security and privacy issues and challenges in Internet of Things," *Int. J. Comput. Sci. Netw. Secur.*, vol. 20, no. 4, pp. 263–286, 2020.
[12] A. Singh and A. Prasher, "Measuring healthcare service quality from patients' perspective: Using fuzzy AHP application," *Total Qual. Manage. Bus. Excellence*, vol. 30, nos. 3–4, pp. 284–300, Feb. 2019.
[13] B. Wang, J. Song, J. Ren, K. Li, H. Duan, and X. Wang, "Selecting sustainable energy conversion technologies for agricultural residues: A fuzzy AHP-VIKOR based prioritization from life cycle perspective," *Resour., Conservation Recycling*, vol. 142, pp. 78–87, Mar. 2019.
[14] M. Yucesan and G. Kahraman, "Risk evaluation and prevention in hydropower plant operations: A model based on Pythagorean fuzzy AHP," *Energy Policy*, vol. 126, pp. 343–351, Mar. 2019.
[15] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017.
[16] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.
[17] J. Granjal, E. Monteiro, and J. S. Silva, "Network-layer security for the Internet of Things using TinyOS and BLIP," *Int. J. Commun. Syst.*, vol. 27, no. 10, pp. 1938–1963, Oct. 2014.

[18] J. Granjal, E. Monteiro, and J. S. Silva, "End-to-end transport-layer security for internet-integrated sensing applications with mutual and delegated ECC public-key authentication," in *Proc. IFIP Netw. Conf.*, 2013, pp. 1–9.
[19] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, "Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures," *ACM Comput. Surv.*, vol. 53, no. 6, pp. 1–37, Feb. 2021.
[20] R. Atiqur, G. Wu, and A. M. Liton, "Mobile edge computing for Internet of Things (IoT): Security and privacy issues," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 18, no. 3, pp. 1486–1493, 2020.
[21] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.
[22] R. Tso, A. Alelaiwi, S. M. M. Rahman, M.-E. Wu, and M. S. Hossain, "Privacy-preserving data communication through secure multi-party computation in healthcare sensor cloud," *J. Signal Process. Syst.*, vol. 89, no. 1, pp. 51–59, Oct. 2017.
[23] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, Jan. 2017.
[24] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT security: Ongoing challenges and research opportunities," in *Proc. IEEE 7th Int. Conf. Service-Oriented Comput. Appl.*, Nov. 2014, pp. 230–234.
[25] A. A. Abdullah and H. U. Khan, "FreGsd: A framework for global software requirement engineering," *J. Softw.*, vol. 10, no. 10, pp. 1189–1198, Oct. 2015.
[26] H. P. Breivold and K. Sandström, "Internet of Things for industrial automation—Challenges and technical solutions," in *Proc. IEEE Int. Conf. Data Sci. Data Intensive Syst.*, Dec. 2015, pp. 532–539.
[27] R. Van Kranenburg and A. Bassi, "IoT challenges," *Commun. Mobile Comput.*, vol. 1, p. 9, Nov. 2012.
[28] A. M. Kozlov, D. Darriba, T. Flouri, B. Morel, and A. Stamatakis, "RAxML-NG: A fast, scalable and user-friendly tool for maximum likelihood phylogenetic inference," *Bioinformatics*, vol. 35, no. 21, pp. 4453–4455, Nov. 2019.
[29] A. A. Zaidan, B. B. Zaidan, M. Y. Qahtan, O. S. Albahri, A. S. Albahri, M. Alaa, F. M. Jumaah, M. Talal, K. L. Tan, W. L. Shir, and C. K. Lim, "A survey on communication components for IoT-based technologies in smart homes," *Telecommun. Syst.*, vol. 69, pp. 1–25, Mar. 2018.
[30] R. Román-Castro, J. López, and S. Gritzalis, "Evolution and trends in IoT security," *Computer*, vol. 51, no. 7, pp. 16–25, 2018.
[31] Y. Yao, J. R. Basdeo, S. Kaushik, and Y. Wang, "Defending my castle: A co-design study of privacy mechanisms for smart homes," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, May 2019, pp. 1–12.
[32] N. Chen and Y. Chen, "Smart city surveillance at the network edge in the era of IoT: Opportunities and challenges," in *Smart Cities*. Binghamton, NY, USA: Springer, 2018, pp. 153–176.
[33] D. Eckhoff and I. Wagner, "Privacy in the smart city—Applications, technologies, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 489–516, 1st Quart., 2018.
[34] Y.-S. Jeong and J. H. Park, "IoT and smart city technology: Challenges, opportunities, and solutions," *J. Inf. Process. Syst.*, vol. 15, no. 2, pp. 233–238, 2019.
[35] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proc. 18th Int. Conf. Eval. Assessment Softw. Eng.*, 2014, p. 38.
[36] M. Niazi, "Do systematic literature reviews outperform informal literature reviews in the software engineering domain? An initial case study," *Arabian J. Sci. Eng.*, vol. 40, no. 3, pp. 845–855, 2015.
[37] M. Niazi, "An exploratory study of software process improvement implementation risks," *J. Soft., Evol. Process*, vol. 24, no. 8, pp. 877–894, Dec. 2012.
[38] S. Siegel, *Nonparametric Stastitics for the Behavioral Sciences*. Washington, DC, USA: American Psychological Association, 1959.
[39] K. B. Wright, "Researching internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services," *J. Comput.-Mediated Commun.*, vol. 10, no. 3, Jun. 2006, Art. no. JCMC1034.
[40] A. Barua, "Methods for decision-making in survey questionnaires based on Likert scale," *J. Asian Sci. Res.*, vol. 3, no. 1, pp. 35–38, 2013.
[41] K. Finstad, "Response interpolation and scale sensitivity: Evidence against 5-point scales," *J. Usability Stud.*, vol. 5, no. 3, pp. 104–110, 2010.
[42] A. A. Khan, J. Keung, M. Niazi, S. Hussain, and A. Ahmad, "Systematic literature review and empirical investigation of barriers to process improvement in global software development: Client-vendor perspective," *Inf. Softw. Technol.*, vol. 87, pp. 180–205, Jul. 2017.
[43] L. M. Rea and R. A. Parker, *Designing and Conducting Survey Research: A Comprehensive Guide*. Hoboken, NJ, USA: Wiley, 2014.
[44] A. A. Khan, J. W. Keung, F. E-Amin, and M. Abdullah-Al-Wadud, "SPI-IMM: Toward a model for software process improvement implementation and management in global software development," *IEEE Access*, vol. 5, pp. 13720–13741, 2017.
[45] C. Noy, "Sampling knowledge: The hermeneutics of snowball sampling in qualitative research," *Int. J. Social Res. Methodol.*, vol. 11, no. 4, pp. 327–344, Oct. 2008.
[46] M. Lewis-Beck, A. E. Bryman, and T. F. Liao, *The SAGE Encyclopedia of Social Science Research Methods*. Newbury Park, CA, USA: Sage, 2003.
[47] S. Easterbrook, J. Singer, M.-A. Storey, and D. Damian, "Selecting empirical methods for software engineering research," in *Guide to Advanced Empirical Software Engineering*. Toronto, ON, Canada: Springer, 2008, pp. 285–311.
[48] M. Bland, *An Introduction to Medical Statistics*. London, U.K.: Oxford Univ. Press, 2015.
[49] M. A. Akbar, J. Sang, A. A. Khan, F.-E. Amin, S. Hussain, M. K. Sohail, H. Xiang, and B. Cai, "Statistical analysis of the effects of heavyweight and lightweight methodologies on the six-pointed star model," *IEEE Access*, vol. 6, pp. 8066–8079, 2018.
[50] I. Keshta, M. Niazi, and M. Alshayeb, "Towards implementation of requirements management specific practices (SP1.3 and SP1.4) for Saudi Arabian small and medium sized software development organizations," *IEEE Access*, vol. 5, pp. 24162–24183, 2017.
[51] S. Mahmood, S. Anwer, M. Niazi, M. Alshayeb, and I. Richardson, "Key factors that influence task allocation in global software development," *Inf. Softw. Technol.*, vol. 91, pp. 102–122, Nov. 2017.
[52] L. A. Zadeh, G. J. Klir, and B. Yuan, *Fuzzy Sets, Fuzzy Logic, and Fuzzy Systems: Selected Papers*, vol. 6. Singapore: World Scientific, 1996.
[53] F. M. Viadiu, M. C. Fa, and I. H. Saizarbitoria, "ISO 9000 and ISO 14000 standards: An international diffusion model," *Int. J. Oper. Prod. Manage.*, vol. 26, no. 2, pp. 141–165, Feb. 2006.
[54] M. B. Ayhan, "A fuzzy AHP approach for supplier selection problem: A case study in a gear motor company," 2013, *arXiv:1311.2886*. [Online]. Available: http://arxiv.org/abs/1311.2886
[55] I. Chamodrakas, D. Batis, and D. Martakos, "Supplier selection in electronic marketplaces using satisficing and fuzzy AHP," *Expert Syst. Appl.*, vol. 37, no. 1, pp. 490–498, Jan. 2010.
[56] D.-Y. Chang, "Applications of the extent analysis method on fuzzy AHP," *Eur. J. Oper. Res.*, vol. 95, no. 3, pp. 649–655, 1996.
[57] D. Stelzer and W. Mellis, "Success factors of organizational change in software process improvement," *Softw. Process, Improvement Pract.*, vol. 4, no. 4, pp. 227–250, Dec. 1998.
[58] L. R. Suzuki, "Smart cities IoT: Enablers and technology road map," in *Smart City Networks*. London, U.K.: Springer, 2017, pp. 167–190.
[59] R. Vinayakumar, M. Alazab, S. Srinivasan, Q.-V. Pham, S. K. Padannayil, and K. Simran, "A visualized botnet detection system based deep learning for the Internet of Things networks of smart cities," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4436–4456, Jul. 2020.
[60] A. R. Javed, Z. Jalil, S. A. Moqurrab, S. Abbas, and X. Liu, "Ensemble AdaBoost classifier for accurate and fast detection of botnet attacks in connected vehicles," *Trans. Emerg. Telecommun. Technol.*, p. e4088, 2020, doi: 10.1002/ett.4088.
[61] S. Sriram, R. Vinayakumar, M. Alazab, and K. P. Soman, "Network flow based IoT botnet attack detection using deep learning," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Jul. 2020, pp. 189–194.
[62] V. Moustaka, Z. Theodosiou, A. Vakali, A. Kounoudes, and L. G. Anthopoulos, "Enhancing social networking in smart cities: Privacy and security borderlines," *Technol. Forecasting Social Change*, vol. 142, pp. 285–300, May 2019.
[63] J. M. de Fuentes, L. Gonzalez-Manzano, A. Solanas, and F. Veseli, "Attribute-based credentials for privacy-aware smart health services in IoT-based smart cities," *Computer*, vol. 51, no. 7, pp. 44–53, Jul. 2018.
[64] A. Anjum, T. Ahmed, A. Khan, N. Ahmad, M. Ahmad, M. Asif, A. G. Reddy, T. Saba, and N. Farooq, "Privacy preserving data by conceptualizing smart cities using MIDR-angelization," *Sustain. Cities Soc.*, vol. 40, pp. 326–334, Jul. 2018.

[65] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, "Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework," *Inf. Syst. Frontiers*, pp. 1–22, 2020, doi: 10.1007/s10796-020-10044-1.
[66] K. Yan, L. Liu, Y. Xiang, and Q. Jin, "Guest editorial: AI and machine learning solution cyber intelligence technologies: New methodologies and applications," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6626–6631, Oct. 2020.
[67] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2671–2701, 3rd Quart., 2019.
[68] H. Larijani, J. Ahmad, and N. Mtetwa, "A heuristic intrusion detection system for Internet-of-Things (IoT)," in *Proc. Intell. Comput. Comput. Conf.*, 2019, pp. 86–98.
[69] L. Ma, A. Y. Teymorian, and X. Cheng, "A hybrid rogue access point protection framework for commodity Wi-Fi networks," in *Proc. 27th Conf. Comput. Commun. (IEEE INFOCOM)*, Apr. 2008, pp. 1220–1228.
[70] W.-L. Chin, W. Li, and H.-H. Chen, "Energy big data security threats in IoT-based smart grid communications," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 70–75, Oct. 2017.
[71] M. Adams, "Big data and individual privacy in the age of the Internet of Things," *Technol. Innov. Manage. Rev.*, vol. 7, no. 4, pp. 12–24, Apr. 2017.
[72] Y. Lu and L. D. Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, Apr. 2019.
[73] T. Varshney, N. Sharma, I. Kaushik, and B. Bhushan, "Architectural model of security threats & their countermeasures in IoT," in *Proc. Int. Conf. Comput., Commun., Intell. Syst. (ICCCIS)*, Oct. 2019, pp. 424–429.
[74] R. S. M. Joshitta and L. Arockiam, "Security in IoT environment: A survey," *Int. J. Inf. Technol. Mech. Eng.*, vol. 2, no. 7, pp. 1–8, 2016.
[75] H. Lin, D. S. Kim, and N. W. Bergmann, "SAGA: Secure auto-configurable gateway architecture for smart home," in *Proc. IEEE 24th Pacific Rim Int. Symp. Dependable Comput. (PRDC)*, Dec. 2019, pp. 1109–1111.
[76] M. Hamza, H. Hu, M. A. Akbar, F. Mehmood, Y. Hussain, and A. M. Baddour, "SIOT-RIMM: Towards secure IOT-requirement implementation maturity model," in *Proc. Eval. Assessment Softw. Eng.*, Apr. 2020, pp. 463–468.
[77] K. Zandberg, K. Schleiser, F. Acosta, H. Tschofenig, and E. Baccelli, "Secure firmware updates for constrained IoT devices using open standards: A reality check," *IEEE Access*, vol. 7, pp. 71907–71920, 2019.
[78] F. J. A. Padilla, E. Baccelli, T. Eichinger, and K. Schleiser, "The future of IoT software must be updated," in *Proc. IAB Workshop Internet Things Softw. Update (IoTSU)*. Dublin, Ireland: Internet Architecture Board, Jun. 2016.
[79] X. He, S. Alqahtani, R. Gamble, and M. Papa, "Securing over-the-air IoT firmware updates using blockchain," in *Proc. Int. Conf. Omni-Layer Intell. Syst.*, May 2019, pp. 164–171.
[80] J. Galeano-Brajones, J. Carmona-Murillo, J. F. Valenzuela-Valdés, and F. Luna-Valero, "Detection and mitigation of DoS and DDoS attacks in IoT-based stateful SDN: An experimental approach," *Sensors*, vol. 20, no. 3, p. 816, Feb. 2020.
[81] F. A. F. Silveira, F. Lima-Filho, F. S. D. Silva, A. de Medeiros Brito Junior, and L. F. Silveira, "Smart detection-IoT: A DDoS sensor system for Internet of Things," in *Proc. Int. Conf. Syst., Signals Image Process. (IWSSIP)*, Jul. 2020, pp. 343–348.
[82] A. Roohi, M. Adeel, and M. A. Shah, "DDoS in IoT: A roadmap towards security & countermeasures," in *Proc. 25th Int. Conf. Autom. Comput. (ICAC)*, Sep. 2019, pp. 1–6.
[83] J. Chen and Q. Zhu, "Interdependent strategic security risk management with bounded rationality in the Internet of Things," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 11, pp. 2958–2971, Nov. 2019.
[84] C.-S. Li, F. Darema, and V. Chang, "Distributed behavior model orchestration in cognitive Internet of Things solution," *Enterprise Inf. Syst.*, vol. 12, no. 4, pp. 414–434, Apr. 2018.
[85] S. Yoon, H. Park, and H. S. Yoo, "Security issues on smarthome in IoT environment," in *Computer Science and Its Applications*. Seoul, South Korea: Springer, 2015, pp. 691–696.
[86] R. K. Kodali and S. Yadavilli, "Mongoose RTOS based IoT implementation of surveillance system," in *Proc. Int. Conf. Commun., Comput. Internet Things (IC3IoT)*, Feb. 2018, pp. 155–158.
[87] J. Wu, C. Wang, Y. Yu, T. Song, and J. Hu, "Sequential fusion to defend against sensing data falsification attack for cognitive Internet of Things," *ETRI J.*, vol. 42, no. 6, pp. 976–986, Dec. 2020.
[88] S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, "Securing the Internet of Things (IoT): A security taxonomy for IoT," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 163–168.
[89] A. Mohanty, I. Obaidat, F. Yilmaz, and M. Sridhar, "Control-hijacking vulnerabilities in IoT firmware: A brief survey," in *Proc. 1st Int. Workshop Secur. Privacy Internet-of-Things (IoTSec)*, 2018, pp. 1–4.
[90] F. Hategekimana, T. J. Whitaker, M. J. H. Pantho, and C. Bobda, "IoT device security through dynamic hardware isolation with cloud-based update," *J. Syst. Archit.*, vol. 109, Oct. 2020, Art. no. 101827.
[91] E. R. Naru, H. Saini, and M. Sharma, "A recent review on lightweight cryptography in IoT," in *Proc. Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC)*, Feb. 2017, pp. 887–890.
[92] Y. Li, S. Ma, G. Yang, and K.-K. Wong, "Secure localization and velocity estimation in mobile IoT networks with malicious attacks," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6878–6892, Apr. 2021.
[93] M. U. Aftab, Y. Munir, A. Oluwasanmi, Z. Qin, M. H. Aziz, Z. Jamali, N. T. Son, and V. D. Tran, "A hybrid access control model with dynamic COI for secure localization of satellite and IoT-based vehicles," *IEEE Access*, vol. 8, pp. 24196–24208, 2020.
[94] B. Pourghebleh, K. Wakil, and N. J. Navimipour, "A comprehensive study on the trust management techniques in the Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9326–9337, Dec. 2019.
[95] M. N. Alraja, M. M. J. Farooque, and B. Khashab, "The effect of security, privacy, familiarity, and trust on users' attitudes toward the use of the IoT-based healthcare: The mediation role of risk perception," *IEEE Access*, vol. 7, pp. 111341–111354, 2019.
[96] X. Zhang, X. Chen, J. K. Liu, and Y. Xiang, "DeepPAR and DeepDPA: Privacy preserving and asynchronous deep learning for industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2081–2090, Mar. 2020.
[97] A. Anand, M. Conti, P. Kaliyar, and C. Lal, "TARE: Topology adaptive re-kEying scheme for secure group communication in IoT networks," *Wireless Netw.*, vol. 26, no. 4, pp. 2449–2463, May 2020.
[98] M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, Jan. 2019.
[99] N. Miloslavskaya and A. Tolstoy, "Internet of Things: Information security challenges and solutions," *Cluster Comput.*, vol. 22, no. 1, pp. 103–119, 2019.
[100] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. Rodrigues, "Authentication in cloud-driven IoT-based big data environment: Survey and outlook," *J. Syst. Archit.*, vol. 97, pp. 185–196, Aug. 2019.
[101] H. Kim and E. A. Lee, "Authentication and authorization for the Internet of Things," *IT Prof.*, vol. 19, no. 5, pp. 27–33, 2017.
[102] D. Rivera, A. García, M. L. Martín-Ruiz, B. Alarcos, J. R. Velasco, and A. G. Oliva, "Secure communications and protected data for a Internet of Things smart toy platform," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3785–3795, Apr. 2019.
[103] H. Aldowah, S. U. Rehman, and I. Umar, "Security in Internet of Things: Issues, challenges and solutions," in *Proc. Int. Conf. Reliable Inf. Commun. Technol.*, 2018, pp. 396–405.
[104] J. M. Corbin and A. Strauss, "Grounded theory research: Procedures, canons, and evaluative criteria," *Qualitative Sociol.*, vol. 13, no. 1, pp. 3–21, 1990.
[105] J. K. W. Wong and H. Li, "Application of the analytic hierarchy process (AHP) in multi-criteria analysis of the selection of intelligent building systems," *Building Environ.*, vol. 43, no. 1, pp. 108–125, Jan. 2008.
[106] S. Soh, "A decision model for evaluating third-party logistics providers using fuzzy analytic hierarchy process," *Afr. J. Bus. Manage.*, vol. 4, no. 3, pp. 339–349, 2010.
[107] E. W. L. Cheng and H. Li, "Construction partnering process and associated critical success factors: Quantitative investigation," *J. Manage. Eng.*, vol. 18, no. 4, pp. 194–202, Oct. 2002.
[108] K. Lam and X. Zhao, "An application of quality function deployment to improve the quality of teaching," *Int. J. Qual. Rel. Manage.*, vol. 15, no. 4, pp. 389–413, 1998.
[109] M. Shameem, R. R. Kumar, C. Kumar, B. Chandra, and A. A. Khan, "Prioritizing challenges of agile process in distributed software development environment using analytic hierarchy process," *J. Softw., Evol. Process*, vol. 30, no. 11, p. e1979, Nov. 2018.
[110] F. T. Bozbura, A. Beskese, and C. Kahraman, "Prioritization of human capital measurement indicators using fuzzy AHP," *Expert Syst. Appl.*, vol. 32, no. 4, pp. 1100–1112, 2007.
[111] T. Yaghoobi, "Prioritizing key success factors of software projects using fuzzy AHP," *J. Softw., Evol. Process*, vol. 30, no. 1, p. e1891, Jan. 2018.

[112] M. Gupta, J. F. George, and W. Xia, "Relationships between IT department culture and agile software development practices: An empirical investigation," *Int. J. Inf. Manage.*, vol. 44, pp. 13–24, Feb. 2019.
[113] K. Kuusinen, P. Gregory, H. Sharp, L. Barroca, K. Taylor, and L. Wood, "Knowledge sharing in a large agile organisation: A survey study," in *Proc. Int. Conf. Agile Softw. Develop.*, 2017, pp. 135–150.
[114] S. Ali and S. U. Khan, "Software outsourcing partnership model: An evaluation framework for vendor organizations," *J. Syst. Softw.*, vol. 117, pp. 402–425, Jul. 2016.

MUHAMMAD AZEEM AKBAR received the M.Sc. and M.S. degrees in computer science from the University of Agriculture Faisalabad (UAF), Faisalabad, Pakistan, and the Ph.D. degree in software engineering from Chongqing University, China. He works as a Postdoctoral Researcher with Nanjing University of Aeronautics and Astronautics, Nanjing, China. He is currently working as a Postdoctoral Researcher with Lappeenranta University of Technology, Lappeenranta, Finland. He has published more than 25 research papers in well-reputed journals and conferences. He has an outstanding academic carrier. His research interests include global software development, requirements engineering, empirical studies, global software requirements change management, software defect prediction, the Internet of Things, code recommender systems, and software risk management and IoT.

AHMED ALSANAD, photograph and biography not available at the time of publication.

SAJJAD MAHMOOD, photograph and biography not available at the time of publication.

ABDULRAHMAN ALOTHAIM, photograph and biography not available at the time of publication.