Neurocomputing 444 (2021) 189–202

Contents lists available at ScienceDirect

Neurocomputing

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

A human-centered artificial intelligence approach for privacy protection of elderly App users in smart cities

Haroon Elahi [a], Aniello Castiglione [b], Guojun Wang [a,*], Oana Geman [c]

[a] School of Computer Science and Cyberengineering, Guangzhou University, Guangzhou 510006, PR China
[b] Department of Science and Technology, University of Naples Parthenope, Isola C4, 80143 Naples, Italy
[c] Health and Human Development Department, Stefan cel Mare University, Suceava 720229, Romania

ARTICLE INFO

Article history:
Received 13 February 2020
Revised 11 June 2020
Accepted 15 June 2020
Available online 26 January 2021

Keywords:
Smart city
Ambient assisted living
Human-centered AI
Privacy as a shared responsibility
Soft sets
Cognitive offloading

ABSTRACT

Artificial Intelligence and Machine Learning based Ambient Assisted Living systems play an important role in smart cities by improving the quality of life of the elderly population. Many Ambient Assisted Living systems are coupled with Android Apps for command-and-control purposes. Consequently, the privacy and security of Ambient Assisted Living systems depend on the privacy and security of the corresponding Android Apps, which follow a privacy self-management model. Unfortunately, the privacy self-management model ignores the decision-making abilities of the elderly and increases their cognitive loads, which put their privacy protection and wellbeing at stake. In this paper, we follow a Human-Centered Artificial Intelligence inspired approach for addressing these issues. This approach uses privacy as a shared responsibility model instead of the privacy self-management model. We have proposed two algorithms, the participatory privacy protection algorithm-I, and participatory privacy protection algorithm-II, for determining optimal privacy settings of an Ambient Assisted Living App and handling its runtime Permission requests, respectively. We demonstrated the working of these algorithms using a case study. We have also compared the proposed approach with state-of-the-art privacy management schemes for Android Apps. The proposed algorithms can improve the privacy protection of Ambient Assisted Living App users in smart cities and relieve them through cognitive offloading.

1. Introduction

By 2050, 16% of the world population will be over the age of 65 [1]. Particularly in Europe and Northern America, by 2050, one in four persons could be aged 65 or over. Since aging introduces different physical and mental impairments, many issues will arise, and health and social care systems will particularly get overburdened [2–4]. Artificial Intelligence (AI) and Machine Learning (ML) based Ambient Assisted Living (AAL) systems can play a significant role in dealing with associated challenges in smart cities of the future [2,5–8].

AAL systems aim to assist the aging population in living a healthier and safer life independently. Provision of context-aware, personalized, adaptive, and anticipatory services, decision support, and aid - when cognitive functions of users decline due to aging - are some of the main functions that AAL systems perform [9] [10]. AAL systems use active and passive sensors, monitoring devices, robotics, and environmental controls embedded in the AAL spaces for sensing data and actuating [4]. AAL systems make intensive use of AI and ML techniques to process the data collected in their operating environments and offer their services to users in a smart city [11].

Contrary to the conventional computing systems, AAL systems lack standard input, output interfaces, and media, e.g., mouse, keyboard, and monitor [2] [12]. Therefore, many AAL solutions depend on devices like Android smartphones for interacting with their users. Not only do numerous Android Apps help AAL inhabitants in solving daily problems, but in many cases, Android Apps can act as command-and-control systems for the AAL systems [6,13,14].

Due to their sensitive nature and potentially vulnerable users, the design, development, and deployment of these systems must consider the specialized needs of their users [15]. For example, the nature of the data that they handle and the functions that they perform affect the well-being of their users and, therefore, make privacy protection a mandatory trait for AAL systems [9] [10,16] [17]. Therefore, specialized privacy-protection controls should be implemented to protect the privacy of the users of AAL systems. However, in general, this is not the case. Research shows that

* Corresponding author.
E-mail address: csgjwang@gzhu.edu.cn (G. Wang).

https://doi.org/10.1016/j.neucom.2020.06.149
0925-2312/

developers of AAL solutions have a minimal consideration of the privacy protections of the users of their products [16].

Likewise, not only does the privacy self-management model in Android ignore the privacy protection needs of potentially vulnerable communities, it increases their cognitive loads. This model requires them to weigh the costs and benefits of the collection, use, and disclosure of their information and decide whether to hold their data or avail the services offered by these App-providers in exchange for their data [18–20]. Moreover, the privacy protection mechanisms in Android do not meet the requirements of AI-based applications [21]. Consequently, the privacy and security risks posed to AAL App users are much significant as compared with ordinary App users.

Fig. 1 shows how an App can ask for access to sensitive data and critical resources on a smartphone. For their privacy protection, users need to be well-versed with Android Permissions, review their options, make decisions, and configure privacy settings of every App that they acquire [22]. Alternatively, they can use the Settings App to configure these settings that require due expertise. A large number of Apps in smartphones, the impact of aging on decision-making ability, lack of awareness of risks of the modern technologies, and cognitive and memory disorders make performing these tasks impossible for AAL users [18,19,23–25]. Finally, the extensive attention needed for performing such complicated tasks increases the cognitive loads of users [26].

Although recent research proposes different decision-support and privacy-management solutions and approaches for App users, they suffer from different limitations due to ignoring cognitive limitations [27,28], and the widespread privacy-incompetence of ordinary users [28–33]. Overall, existing approaches ignore the needs of AAL App users.

The purpose of conducting this research is to improve the privacy protection of AAL App users in smart cities while relieving them from cognitive loads resulting from complex decision-making associated with the privacy self-management model. We follow a Human-Centered Artificial Intelligence (HCAI) based approach and offer two algorithms for determining the optimal privacy settings of AAL Apps. HCAI advocates that AI and ML algorithms in interactive intelligent systems should consider the fact that they are part of larger systems involving humans [34]. We treat achieving optimal privacy settings of an AAL App as a multi-criteria decision-making (MCDM) problem and use soft sets to solve this problem. Soft sets are specialized tools for designing solutions dealing with MCDM under uncertainty [35,36],37.

Following an HCAI-based approach, to achieve the goal of improving the privacy protection of AAL App users in smart cities while relieving them of cognitive loads resulting from the complex decision-making associated with the privacy self-management model, this research makes the following contributions.

(1) It is the first work that focuses on improving the privacy protection of elderly users in smart cities by determining the optimal privacy settings of Android Apps used for user-interaction and command and control by AAL systems. We use an HCAI-based approach for improving the privacy protection of Android App users in AAL spaces. In our approach, we integrate privacy as a shared responsibility model and propose using the decisions and preferences of expert Android users for determining the privacy settings of AAL apps.
(2) We use the soft set theory for modeling and evaluating the decisions and preferences of expert users finding optimal privacy protection settings of AAL Apps. Soft sets can handle multi-value input and uncertainty better than probabilistic approaches [38]. However, so far, they have not been used for designing solutions for privacy-related problems.

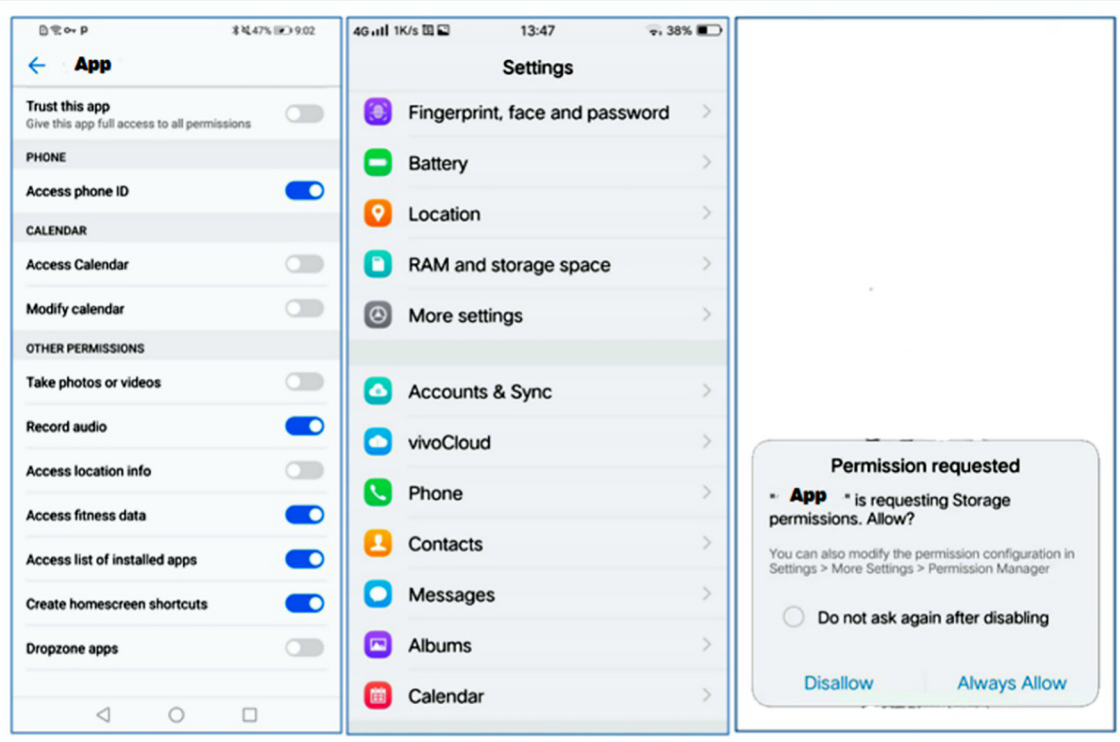

Fig. 1. (Left) A simple App is accessing sensitive information. The settings of the App contain a "Trust this App" option that, if selected, enables an App to gain full access to all requested Permissions. (Center) A Settings App can help in managing privacy settings of Apps installed on an Android smartphone. (Right) A runtime Permission request. It gives users three options, "disallow," "always allow," and "do not ask after disabling.".

(3) We propose two algorithms, participatory privacy protection algorithm - I (PPPA-I) and participatory privacy protection algorithm - II (PPPA-II), for the privacy protection of elderly Android App users in smart cities. PPPA-I solves the problem of determining the optimal privacy settings of an App, and PPPA-II handles the Dangerous Permission requests of AAL Apps at the runtime. Together, the proposed algorithms automate privacy management and achieve cognitive offloading by relieving AAL App users of the burden of complex decision-making needed for privacy self-management.
(4) We demonstrate the working of the proposed approach and algorithms by conducting a user study to collect data from twenty expert Android users and using a popular messenger App as a case study.

The rest of the paper organizes as follows. Section 2 introduces essential background concepts. Section 3 formulates the problem. Section 4 offers the proposed approach, and Section 5 proposes two algorithms. Section 6 provides a demonstration of the working of the proposed approach through a case study. Section 7 compares the proposed approach with state of the art and discusses its different implications. Section 8 discusses different limitations of this work. Section 9 provides an overview of the related work. Finally, Section 10 concludes this paper.

2. Background

In this section, we introduce the notions of HCAI and privacy as a shared responsibility and then provide some preliminaries and definitions.

2.1. Human-centered Aritificial Intelligence (HCAI)

Intelligent systems involving human/machine interaction are known as human-centered intelligent systems [39]. Human-centered artificial intelligence (HCAI) advocates that the design of human-centered intelligent systems and their underlying AI and ML algorithms should consider the fact that they will be part of systems, including humans [34]. HCAI proposes that algorithms for human-centered intelligent systems should have attributes such as fairness, transparency, accountability, and explainability, etc.

2.2. Privacy as a Shared Responsibility

Privacy as a shared responsibility assigns individuals the responsibility to protect their own and others' privacy. Australian Law Reform Commission [40] notes 'provided they have the power and means to do so, individuals bear a measure of responsibility for the protection of their own privacy and the privacy of others.' Thus App providers, App users, advertisers, legislators, designers, and any other stakeholders involved in the business must accept their responsibility to protect privacy, their own, and of others.

2.3. Soft Set

Let X be an initial universe set and E be a non-empty set of parameters. Then a soft set can be defined as follows.

A pair (F, E) is called as a soft set over X, if and only if F is a mapping from E into $P(X)$, the set of all subsets of X.

$$F : E \mapsto P(X) \tag{1}$$

Therefore, soft set can also be considered as a parameterized family of subsets of the universe X [38,41].

As given in [42], if X is the universe, then it comprises of objects under consideration, and E - the set of parameters, comprises of different words or sentences representing their values. For example, suppose that X is the set of privacy decisions of Android users that need to be evaluated, and E is the set of levels of preferences expressing whether a Permission is needed for the functions of an App or not. In this case, defining soft sets will mean pointing out specific decisions from X according to various values of E assigned by the users, and a soft set (F, E), in this case, will describe the preferred decisions of users to allow or deny given Android Permissions to an App for its functions.

2.4. Knowledge Representation System

A soft set can be considered as a knowledge representation system that represents some data regarding the universal set X with respect to a set of parameters E [43]. The formal definition, as given in [35] is provided below.

Let X be a non-empty finite set called as Universe and E be a non-empty finite set of primitive parameters, then a pair $S = (X, E)$ will be called as a knowledge representation system such that:

$$e \in E \tag{2}$$

And

$$e : X \mapsto V_e \tag{3}$$

Where V_e is a set of values of e and is called as the domain of e.

2.5. Tabular Presentation of Soft Set

A soft set can be presented in a tabular form, as shown in [35], [44,45]. For example, if (F, E) is a soft set, defined over a set of parameters E, then we can present this soft set as shown in Table 1.

In Table 1, $e_j (j = 1, 2, \ldots, 5)$ are the elements of E. An element of the Table 1 y_{ij} is one if $x_i \in F(e_j)$, otherwise it is zero.

2.6. Adding Row and Column Entries

If a table representing a soft set has $I = 1, 2, 3, \ldots, m$ rows and $J = 1, 2, 3, \ldots, n$ columns, the row-sum r_i and the colum-sum t_j can be calculated as following.

$$r_i = \sum_{j=1}^{n} y_{ij} \tag{4}$$

$$t_j = \sum_{i=1}^{m} y_{ij} \tag{5}$$

2.7. Choice Value of a Decision

The choice value of a decision $x_i \in X$ can be denoted by c_i and can be calculated as following [35].

Table 1
Tabular Presentation of a Soft Set.

X\E	e_1	e_2	e_3	e_4	e_4
x_1	1	1	1	1	1
x_2	1	1	1	0	1
x_3	0	0	1	1	1
x_4	0	1	1	1	0
x_5	0	1	1	1	1

$$c_i = \sum_j y_{ij} \tag{6}$$

Where y_{ij} are the entries of the tabular form of the soft set, and i and j represent rows and columns, respectively.

2.8. Weighted Table of Soft Set

A weighted table of a soft set contains weighted entries of the parameters [35]. Thus, instead of y_{ij}, the entries take the form of $d_{ij} = w_{ij} \times y_{ij}$, where i and j represent rows and columns, respectively.

2.9. Weighted Choice Value

Weighted choice value of decisions made by the users can be calculated as following.

$$c_{wi} = \sum_j d_{ij} \tag{7}$$

2.10. Subjective Weights

Weights reflect the relative importance of different attributes [36]. In the case of privacy decisions, subjective weights are reflected by the preferences of users and a subjective weighting method can be used to learn the relative privacy preferences of users. Such weights can reflect relatively high or relatively low preferences of users.

Subjective weights are calculated using the following equation [36].

$$W = 1/n(\sum_{j=1}^{n} w_j^p) \tag{8}$$

Where $j = 1, 2, \ldots, n$ and w_j^p is weighted choice values of jth parameter.

2.11. Multi-Criteria Decision Making

In the case of MCDM, a user is encountered with a set of alternatives D and he or she is needed to reach an optimal decision d_{opt} [46]. In order to achieve this, he or she evaluates a set of parameters (criteria) $P = \{p_1, p_2, \ldots, p_i, \ldots, p_n\}$ and p_i can have a single value from a set of values $E = \{e_1, e_2, \ldots, e_j\}$ where $j \geqslant 2$ and each value represents a different degree of importance/preference. A user tries to come up with an optimal decision d_{opt} such that he or she selects a set of x parameters $P_x \subseteq P$ where $x \leqslant n$, each having a value e_y such that $e_y \in E$.

3. Problem Formulation

We understand that the problem of determining optimal privacy settings of an App during the privacy self-management is an MCDM problem. Considering the problem of finding optimal privacy settings of an AAL App, let $X = \{d_1, d_2, d_3, \ldots, d_n\}$ be a set of n alternatives (e.g., decisions made by experts) that need to be evaluated, $E = \{e_1, e_2, e_3, \ldots, e_m\}$ be the set of parameters involved in the decisions, and $E_y = \{very\ low, low, medium, high, very\ high\}$ be the set of potential values that an expert user can assign for expressing his or her preference to a parameter $e_i \in E$. Then a soft set (F, E) which describes a certain level of willingness of experts to allow or deny Permissions can be written as $F : E \mapsto P(X)$ where $P(X)$ is the power set of X, and E is the set of permissions. Permissions are strings of text that control an App's access to sensitive data and critical resources in an Android smartphone. A user may or may not consider a permission necessary for the functions of an application. The level of necessity is described by the user's preference. Therefore, $F(e)$ for $e \in E$ may be empty in some cases. This will be when a user considers that this permission is not needed for any of the given functions.

Looking at the nature of the problem, it is evident that it requires extensive attention and memory usage. Such problems increase the cognitive load of decision-makers [26]. Older adults, living in AAL spaces in smart cities, can suffer from different cognitive impairments [19,18]. Not only can such decision-making requirements result in errors leading to the sub-optimal configuration of privacy settings, but they can affect the mental well-being of these users.

4. The Proposed Approach

Keeping in view the architecture of AAL systems and underlying AI and ML technologies, we follow an HCAI-based approach for improving the privacy protection of AAL App users in Smart cities. HCAI focuses on the design, development, and deployment of AI and ML algorithms for the environments that may involve direct human interaction [34]. We modify a previously proposed approach in [47] and align it with the requirements of AAL spaces and users. Further, cognitive offloading can be achieved by reducing user interaction during privacy management [48]. Fig. 2 provides an overview of the proposed apporach. Our approach has the following steps.

4.1. Participatory Privacy Testing

We use participatory privacy testing (PPT) for noting the decisions and preferences of expert Android users. PPT is the set of data collection tools and procedures used to learn the decisions and preferences of users as they evaluate the functions of a given

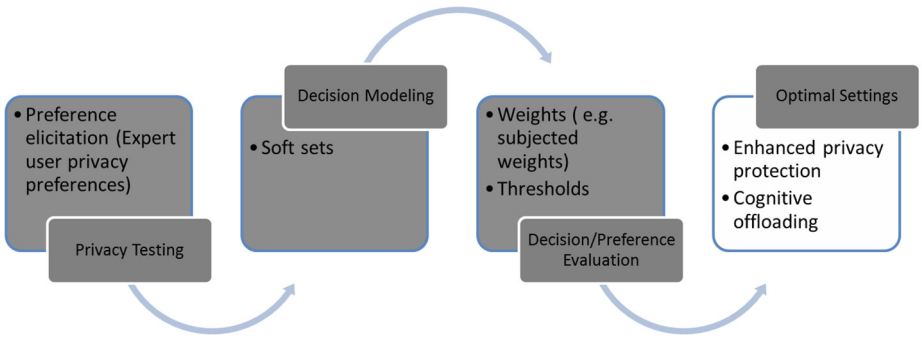

Fig. 2. An overview of the proposed approach.

App, e.g., deciding whether requested Permissions are needed for the given functions [47].

Since AAL App users are unable to engage in complex decision-making due to their cognitive limitations, we maintain that in this case, privacy self-protection model fails, and privacy protection in AAL spaces becomes a shared responsibility. Therefore, we propose to use the decisions and preferences of expert users for the privacy protection of AAL App users. Engaging experts to evaluate ML-based solutions and collecting the evaluation data is a known practice [49]. Likewise, different researchers have involved experts in designing solutions for AAL spaces, such as personalization of remote assistance Apps for the elderly [50]. However, in current research, we engage expert Android users to learn their decisions and preferences for determining the privacy settings of Apps used in AAL spaces.

4.2. Decision/Preference Modeling

Data collected during the PPT need to be structured in an adequate format so that a privacy management system can process them. Privacy decisions are subject to factors like bounded rationality and incomplete information that introduce uncertainty in the decision making process [24,51]. Therefore, decision and preference data need to be modeled using a tool that may handle underlying uncertainty. We apply the soft set theory to model the decisions and preferences of expert users. Soft sets are a suitable tool for modeling decisions under uncertainties [35,43]. Other tools available for dealing with problems involving uncertainty include the theory of probability, theory of fuzzy sets, and the interval mathematics. However, these theories have their limitations [38]. For example, the theory of probability can deal only with stochastically stable phenomena. It also becomes computationally expensive for its data-intensive nature [52]. Interval mathematics is not sufficiently adaptable in cases where uncertainty is variable. Setting the membership function in different cases when using fuzzy sets is an open problem.

4.3. Decision/Preference Evaluation

Different decisions of expert users for determining optimal privacy settings of Apps need to be evaluated for finding the optimal settings. We propose the use of weighted choice values and subjective weights for comparing decisions and preferences. Weighted choice values can help in ranking the decisions. The subjective weights can determine relative importance according to preference or judgment of expert users [36,53]. Likewise, threshold values can be used for filtering sub-optimal decisions. Similar metrics have been used in the past while dealing with complex decision-making problems [35]. Recent research validates the effectiveness of this approach in related problems [54].

In the following section, we use our approach for designing two algorithms.

5. Proposed Algorithms

We propose the two algorithms, Participatory Privacy Protection Algorithm–I (PPPA-I) and Participatory Privacy Protection Algorithm-II (PPPA-II), to determine optimal privacy settings of an App and for handling runtime Dangerous Permission requests, for enhancing the privacy protection of AAL inhabitants and relieving them of cognitive loads introduced by privacy self-management.

Algorithm 1: Participatory Privacy Protection Algorithm-I (PPPA-I)

1: **Input:** *Expert decisions (X) (over Permissions (E) of an App for the given functions), A threshold value (λ)*
2: **Output:** *Optimal privacy settings*
3: **Steps**:
4: Define the soft set (F, E)
5: Input the set of choice parameters of experts, which are subset of E
6: Ignore the choice parameters, that more than 50% experts consider unnecessary
7: Find weighted table of the soft set (F, E) according to the weights assigned by the experts
8: Calculate weighted choice value (c_{wi}) for each decision (x_i) using Eq. 7
9: Find k, for which c_{wi} is the minimum (c_{wmin}). k represents optimal decision
10: Apply a threshold value (λ) to further remove Permissions

Algorithm 2: Participatory Privacy Protection Algorithm-II (PPPA-II)

1: **Input:** *Requested Permission (p_i), Expert user preferences (E) for p_i, Threshold value (λ_i)*
2: **Output:** A Binary Decision Value
3: **Steps**:
4: Define the soft set (F, E)
5: Input the set of choice parameters of experts, which are subset of E
6: Find weighted table of the soft set (F, E) according to the preferences of the experts
7: Calculate the subjective weight (W) for the Permission p_i using Eq. 8
8: If the subjective weight of user preferences for Permission p_i is more than the threshold value (λ_i), allow, otherwise, deny

5.1. PPPA-I

Participatory Privacy Protection Algorithm –I (PPPA-I) takes input in the form of expert user decisions (X) regarding the requested Permissions (E) against given functions of an App and records their preferences (E_y) regarding the extent to which a particular Permission is needed. It also takes a threshold value (λ) that is used for final evaluation purposes. PPPA-I algorithm evaluates expert decisions and uses weighted choice values (c_{wi}) and thresholds to identify the optimal settings. Weighted choice value (c_{wi}) can vary from choice-value (c_i) depending upon an expert's perception of the degree of necessity for different Permissions for performing described tasks. The threshold values (λ) for different Permissions can be set by the moderators, app designers, or privacy controllers.

5.2. PPPA-II

The Participatory Privacy Protection Algorithm – II (PPPA-II) solves the problem of handling the Dangerous Permission requests

of an App at the runtime. It takes the privacy preferences of Expert Android users (E) regarding a particular Permission (p_i) and a threshold value (λ_i) as inputs. It uses soft sets theory to model the preferences and calculates subjective weights (W) of Permission preferences assigned by expert users to decide at runtime whether to allow or deny Permission (p_i). The threshold value (λ_i) is used for making the final decision. The threshold value (λ_i) for different Permissions can be set by the moderators, app designers, or privacy controllers. This algorithm intends to relieve AAL App users of the cognitive loads resulting from the runtime Permission handling.

6. Case Study

We conducted a user study to collect data to demonstrate the working of the proposed approach for the privacy protection of Android users belonging to vulnerable communities such as older adults living in AAL spaces.

6.1. Data Collection

We had to learn the decisions and preferences of expert Android users while setting the privacy settings of an Android app. We assumed that Android users with Android development experience had a better ability to understand the functional description of an app than those users who had no such experience. This assumption was based on the fact that software developers regularly engage in understanding app requirements [55]. We selected a messenger app for evaluation by expert users and recruited twenty Android users with Android development experience from three software houses in Pakistan. Some other research works on AAL issues have also engaged domain experts for solution design [9,50]. We designed a survey instrument for data collection (the content of the survey instrument is provided in A).

6.2. Demographics

In total, there were twenty participants in this study. There were fifteen males and five females among the participants. The average age was 25 years, with a standard deviation value of 3, and the average experience was 2.3 years with a standard value of 1.7.

6.3. Procedure

We selected one of the most widely used messenger Apps as a case study for demonstration purposes. A vast majority of users use messengers, and even those in AAL spaces can use them for communicating with peers, health staff, and family members [6,56]. We picked the description of the selected messenger App from Google Play Store and anonymized it. Permissions that it asks from users to be allowed were also noted. We offered the description and the associated Permissions to the participants in our study. If a participant thought that given Permission was needed for the functions of the messenger App, he or she would further select a value from 'very low,' 'low,' 'medium,' 'high,' and 'very high' to express the perceived degree of necessity of this Permission for the given functions.

6.4. Choosing Optimal Privacy Settings of an App

We used Participatory Privacy Protection Algorithm-I (PPPA-I) for this purpose. The steps were as following.

6.5. Defining Soft Sets

We define the soft set $F(E)$ over the universal set $X = \{h_i\}$. Where $h_i = 1, 2, \ldots, m$ are decision alternatives. And $E = \{p_1, p_2, \ldots, p_n\}$ are the set of Permissions.

6.6. Tabular Presentation of Data

Table 2 models the decisions of twenty users in tabular form. The values in the rows i.e., 1 or 0 represents whether a user considers that this particular Permission is needed for the given functions in the App description. Applying a majority vote, the Permissions considered needed by less than 50% of users can already be removed before further processing. These Permissions should never be considered for options like 'allowed always' and everytime an App must seek user consent.

For example, only three out of twenty participants deem p_1 necessary for performing functions listed in the description. Similarly, only seven participants consider p_2 necessary and so on. In this process, we remove $p_1, p_2, p_{10}, p_{11}, p_{12}, p_{13}$, and p_{18}.

Table 2
Tabular Presentation of Data Collected from Twenty Experts.

X\E	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}	p_{12}	p_{13}	p_{14}	p_{15}	p_{16}	p_{17}	p_{18}
h_1	0	1	0	1	1	1	0	1	1	0	0	1	1	1	0	1	1	1
h_2	0	0	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	0
h_3	0	0	0	1	1	1	1	1	1	0	0	0	0	1	1	1	1	0
h_4	0	0	1	1	1	1	0	0	1	0	0	0	1	1	1	1	1	1
h_5	0	0	1	1	1	1	1	1	1	0	0	0	1	1	1	1	1	0
h_6	0	0	1	1	1	1	0	1	1	0	0	0	0	1	1	1	1	0
h_7	0	0	1	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0
h_8	0	0	1	1	1	1	1	1	1	0	0	0	0	1	1	1	0	0
h_9	0	0	1	0	1	1	0	0	1	0	0	0	0	1	1	1	1	0
h_{10}	0	0	0	1	1	1	0	0	1	0	1	0	0	1	1	1	0	0
h_{11}	0	1	1	1	1	1	0	1	1	0	0	0	0	1	1	1	1	1
h_{12}	0	0	0	1	1	1	0	1	1	0	0	0	0	1	1	1	1	0
h_{13}	0	0	1	1	1	1	0	0	1	0	0	0	0	1	1	1	1	0
h_{14}	0	0	0	1	1	1	0	1	1	0	1	0	0	1	1	1	1	1
h_{15}	0	1	0	1	1	1	1	1	1	0	0	0	0	1	1	1	1	0
h_{16}	0	0	0	1	1	1	0	1	1	0	0	0	0	1	1	1	1	1
h_{17}	1	1	1	1	0	1	1	1	1	1	0	0	0	0	0	0	0	1
h_{18}	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1
h_{19}	1	1	1	1	0	1	1	1	1	1	1	1	0	0	0	0	0	0
h_{20}	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1

6.7. Preparing Weighted Table of the Soft Sets

In this step, we replace all ones with the actual weights assigned by the users describing their relative importance for performing given functions. Users had options 'very low,' 'low,' 'medium,' 'high,' and 'very high.' We replace them with '0.1,' '0.3,' '0.5,' '0.7,' and '0.9,' respectively. These weights can be assigned according to the relative importance of different parameters values [57]. Table 3 shows the weighted table of soft sets.

6.8. Calculating Weighted Choice Values (c_w)

We calculate weighted choice value (c_w) for each decision using Eq. 7. The last column of Table 3 shows the c_w of decisions.

6.9. Finding k with Minimum c_w

The decision with minimum weighted choice value (c_w) will ensure maximum privacy. For example, in the Table 3, the weighted choice value (c_w) of d_{20} is 0.9, which means that this is the optimal decision and only one permission p_3 should be considered for options like 'allowed always.'.

6.10. Applying Thresholds

Even though decision with minimum weighted choice value (c_{wmin}) is optimal decision for privacy detection, a threshold value (λ) can be applied for further optimzation. For example, in Table 3, if d_8 turns out to be the optimal decision, applying a threshold of 'very high' will remove p_3 and p_4.

6.11. Runtime Permission Management

From Android 6.0 onwards, Android Apps are required to ask for user permission to access sensitive data and critical device resources at the runtime when they need to access such data or resources. During runtime Permission management, an App prompts a user to approve or reject a single Permission. Due to the lack of awareness, the user may not be able to rationally evaluate a given Permission and make a wrong decision [58]. We use the second algorithm - Participatory Privacy Protection Algorithm - II (PPPA-II) to determine whether to allow or deny a given Permission to an App at the runtime. We explain this approach using the example of p_3 in Table 3.

6.12. Defining Soft Set

In this case, we evaluate the Permission p_3 against the decisions of experts and their preferences. $X = \{p_3\}$ and $E = \{u_1, u_2, \ldots, u_{20}\}$. Each user u_i can assign values {very low, low, medium, high, very high}.

$F(p_3) = \{u_2, u_4, u_5, u_6, u_7, u_8, u_9, u_{11}, u_{13}, u_{17}, u_{18}, u_{19}, u_{20}\}$

6.13. Tabular Presentation of Soft Sets

Table 4 shows the tabular presentation of expert user for approval or denial of p_3.

6.14. Weighted table

Table 5 shows the weighted choices (c_w) or preferences of users regarding approval or denial of p_3.

6.15. Calculating Subjective Weight (W)

Subjective weight (W) for p_3 is calculated using the Eq. 8. The subjected weight amounts to 0.62.

6.16. Applying Thresholds

If a threshold value (λ) of 'high' is applied, p_3 will be denied. However, if threshold value (λ) of 'medium' is applied, p_3 will be granted to the app.

Table 3
Weighted Table of Data and Weighted Choice Values(c_{wi}).

X\E	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{13}	p_{14}	p_{15}	p_{16}	p_{17}	c_w
d_1	0	0.7	0.7	0.9	0	0.7	0.9	0.7	0.3	0	0.9	0.7	6.5
d_2	0.7	0.7	0.7	0.9	0.9	0.9	0.7	0	0.9	0.9	0.9	0.9	9.1
d_3	0	0.7	0.9	0.9	0.9	0.9	0.9	0	0.9	0.9	0.9	0.9	8.8
d_4	0.7	0.9	0.9	0.9	0	0	0.9	0.5	0.9	0.9	0.9	0.9	8.4
d_5	0.5	0.7	0.9	0.9	0.9	0.9	0.9	0.7	0.9	0.9	0.9	0.9	10
d_6	0.7	0.7	0.9	0.9	0	0.7	0.7	0	0.9	0.9	0.9	0.9	8.2
d_7	0.7	0.7	0.9	0.9	0	0.9	0.9	0.5	0.9	0.9	0.9	0.9	9.1
d_8	0.5	0.5	0.9	0.9	0.9	0.9	0.9	0	0.9	0.9	0.9	0	8.2
d_9	0.9	0	0.9	0.9	0	0	0.9	0	0.9	0.9	0.9	0.9	7.2
d_{10}	0	0.9	0.9	0.9	0	0	0.9	0	0.9	0.9	0.9	0	6.3
d_{11}	0.3	0.7	0.9	0.9	0	0.7	0.9	0	0.9	0.9	0.9	0.9	8
d_{12}	0	0.9	0.9	0.5	0	0.7	0.9	0	0.9	0.9	0.9	0.9	7.5
d_{13}	0.7	0.9	0.9	0.9	0	0	0.9	0	0.9	0.9	0.9	0.9	7.9
d_{14}	0	0.7	0.9	0.9	0	0.7	0.7	0	0.9	0.9	0.9	0.9	7.5
d_{15}	0	0.9	0.9	0.9	0.7	0.7	0.7	0	0.9	0.9	0.9	0.9	8.4
d_{16}	0	0.9	0.9	0.9	0	0.9	0.9	0	0.9	0.9	0.9	0.9	8.1
d_{17}	0.7	0.7	0	0.7	0.7	0.7	0.9	0	0	0	0	0	4.4
d_{18}	0.3	0.5	0.5	0.7	0.7	0.9	0.9	0.5	0.5	0.7	0.7	0.3	7.2
d_{19}	0.5	0.5	0	0.7	0.7	0.7	0.5	0	0	0	0	0	3.6
d_{20}	0.9	0	0	0	0	0	0	0	0	0	0	0	0.9

Table 4
Tabular Presentations of User Preferences for Approving p_3.

X\E	u_2	u_4	u_5	u_6	u_7	u_8	u_9	u_{11}	u_{13}	u_{17}	u_{18}	u_{19}	u_{20}
p_3	1	1	1	1	1	1	1	1	1	1	1	1	1

Table 5
Weighted Table of User Preferences for Approving p_3. The last column contains subjective weight (W).

X\E	u_2	u_4	u_5	u_6	u_7	u_8	u_9	u_{11}	u_{13}	u_{17}	u_{18}	u_{19}	u_{20}	W
p_3	0.7	0.7	0.5	0.7	0.7	0.5	0.9	0.3	0.7	0.7	0.3	0.5	0.9	0.62

7. Discussion

The integration of AAL systems with Android Apps for user interaction and command-and-control purposes offers the privacy management challenges beyond the competence and abilities of inhabitants of AAL spaces. Factors like potential cognitive impairments of the AAL inhabitants, the number of Apps installed on phones, a large number of Permissions involved in their privacy management, and the screen size and the complexity of interface design make achieving adequate privacy protection quite complicated for these users [23,59–61]. Consequently, AAL inhabitants are burdened with cognitive loads that put their well-being at risk, and AAL Apps can get unobtrusive access to sensitive user data and critical device resources. This allows possibilities of privacy violations of their users and the AAL systems [62–65].

Subsequently, in AAL spaces, the prevailing 'privacy as a control' approach fails due to the inability of AAL inhabitants to meet the requirements of the privacy self-management model. The 'privacy as a shared responsibility' approach that is mostly missing in scholarly literature is a practical solution for this problem. This approach advocates that all stakeholders should accept their responsibility in protecting the privacy of users [18]. In this paper, we adopted an HCAI-inspired participatory approach for improving the privacy protection of older App users in smart cities. The proposed approach integrates the privacy as a shared responsibility model and takes advantage of the participation of expert Android users, learns their decisions and preferences, and applies it to improving the privacy of AAL inhabitants, achieving cognitive offloading by removing the requirement of user interaction.

Preference modeling is one of the biggest challenges in ambient intelligence systems, and the techniques generally used cannot handle uncertainty [66]. The uncertainty makes this preference modeling tremendously tricky. Soft sets are known to be a powerful tool for dealing with uncertainty [42]. While conventional methods, such as theory-based probability methods and support vector machines (SVMs), when used to deal with problems involving uncertainty, need an exact model in the beginning and return an approximate output, soft sets start with an approximate model and provide a crisp output [38,67,68].

We proposed two algorithms (PPPA-I and PPPA-II) to achieve optimal privacy settings for Android Apps used in AAL spaces while relieving AAL users of complex decision-making tasks. These algorithms apply soft set theory for decision and preference modeling and evaluation. We have demonstrated that these algorithms could effectively model the decisions of expert Android users and their preferences and use different soft set operations to determine optimal privacy settings of an App and manage runtime Permissions, respectively.

As shown in Table 6, when compared with state of the art privacy management and protection techniques for users, the proposed approach has many strengths. It is participatory, non-privacy-invasive, does not require user interaction at runtime, uses a decision and preference modeling approach that is deemed most suitable for decision making under uncertainties, and mainly serves the needs of AAL Android users. Contrary to most of the existing approaches that involve ordinary users, who are known to lack privacy awareness, the proposed approach involves expert users [30,28,32,71].

If we compare the proposed approach with the only privacy modeling computation and management scheme for AAL users [69], it has three main advantages. First, it involves expert users; second, it focuses on AAL Apps rather than IoT equipment in AAL spaces; and it relieves users from the complex decision making required for managing privacy settings of Apps and handling runtime Permissions. Also, the previously proposed scheme in [69] still depends upon users' 'willingness' to release or hold data, a requirement unreasonable for the abilities of AAL users.

The proposed approach and algorithms achieve cognitive offloading by relieving AAL users in the smart city from the burden of complex decision making required for risk assessment and reduce associated risks through automatic privacy management in AAL Android Apps. Such automatic risk assessment of mobile systems is a long-desired trait [72]. Recent research suggests that Android security mechanisms do not meet the privacy protection requirements of Apps integrating AI and ML [21]. The proposed algorithms can be used in the privacy management systems to deal with privacy settings and runtime Permissions of such Apps.

The automation of privacy management in Android smartphones, even if partial, can draw criticism. For example, recent research focusing on informed consent suggests that requirements of free consent in the European Union's General Data Protection Regulation (GDPR) [73] hinders automating the consent [10]. However, GDPR, in directive 36, says, "The measures taken by the controller should include drawing up and implementing specific safeguards in respect of the treatment of personal data of vulnerable natural persons, such as children." We believe that assuming the shared responsibility of protecting the privacy of vulnerable communities, such as AAL inhabitants, is a desirable safeguard needed to ensure their privacy protection.

Past research proposes implementing marketplace-level privacy protection solutions for the adequate privacy protection of Android users [74]. We argue that involving all stakeholders, including users or expert users, App developers, the marketplace, and the regulators can ensure improved privacy protection of App users in general, and the vulnerable communities such as older smartphone users living in AAL spaces, in particular. While

Table 6
Comparison with State-of-the-Art.

Approach	Involves Users?	Privacy Invasive?	Needs User Interaction?	Underlying Methods?	Target Audience
PMD & AID-S [32]	Yes	Yes	Yes	Bayesian Network	Fitness App Users
Segmentation [30]	Yes	No	Yes	Segmentation Methods	OSN (FB) Users
Privacy Setting Prediction [28]	Yes	No	Yes	Support Vector Machines	Online Service Users
Privacy Settings Model [31]	Yes	No	Yes	Correlation	OSN Users
Setting Default Settings [47]	Yes	No	No	Simple Averages	General App Users
Privacy Management Approach [69]	Yes	No	Yes	Decision Matrices	AAL Inhabitants
SecuRank [70]	No	Yes	Yes	Cosine Similarity	General App Users
The Proposed Approach	Yes	No	No	Soft Sets	AAL inhabitants

the proposed approach to privacy protection can reduce the burden imposed by the privacy self-management model by semi-automating privacy protection, at the same time, it distributes the privacy protection responsibility among different stakeholders.

Our research also highlights the importance of considering the privacy protection needs of vulnerable communities, such as older adults living in AAL spaces while designing respective controls. However, contrary to the research that advocates personalization of privacy [30] or embedding the preferences of AAL users in the AAL Apps and solutions [50,66], we propose that when it comes to the privacy of these users, the privacy protection solutions should also consider their physical and mental limitations. Approaches like adapting to the preferences of expert users can be more effective in such cases. Contrarily, building privacy protection systems learning from the decisions and preferences or AAL users can potentially bring havoc due to the limitations of these users.

In the end, realtime access control is a challenge in many domains, and configurable and auto-configurable methods are needed to face this challenge [75,65,76,77]. Our proposed algorithms make contributions to the research in this direction by demonstrating the runtime Dangerous Permission management.

8. Limitations

In this section, we discuss the different limitations of this work. In this research, we have involved only twenty experts while evaluating the App functions and its Permission requirements to determine optimal privacy settings. This is mainly due to presentation reasons. Moreover, the use of expert reviews is a known method, and one of its strengths is that a few expert users can help in achieving the desired goals by producing quality information [78,79].

Recruiting expert users for recording the decisions and preferences can be challenging. Previous research suggests maintaining a pool of representative users for accessibility research due to challenges faced in recruiting representative users in a timely fashion [80]. We propose that keeping in view the sensitivity of privacy protection of AAL users, a similar approach can be used, and a pool of expert users can be maintained by professional or regulatory bodies responsible for the well-being of older adults in the smart cities.

Further, we have involved Android developers and assumed that they are better than ordinary Android users at evaluating App descriptions and their Permission demands to determine whether the asked Permissions match given functions. Although some works criticize that the privacy expectations of developers may differ from those of ordinary users [81], in our approach, we assume that vulnerable communities lack an understanding of privacy management mechanisms. Further, previous research shows that even ordinary Android users lack the awareness and skills needed for effective privacy management [58]. However, privacy-aware domain experts such as AAL experts and health professionals can be involved to generate a more reliable dataset.

Lastly, assisted privacy management may appear to reduce the control of AAL users over their privacy. However, for users who have the needed levels of privacy-awareness and skills can always use the ‘Settings App’ provided in Android smartphones for adjusting App settings. Simultaneously, the proposed approach can shield those who do not possess the traits needed for effective privacy self-management.

9. Related Work

In this section, we provide a brief review of the related works on privacy issues in AAL spaces, privacy settings of Android apps, and the use of soft sets in addressing the related problems.

9.1. Privacy Issues in AALSpaces

Privacy issues in AAL systems can affect the privacy, safety, and well-being of the aging population in smart cities. Consequently, we see that recently different researchers have focused on related problems. M.E. Moris et al. [4] found that addressing privacy issues in AAL systems was one of the pre-conditions for their acceptance by the potential users. Skouby et al. [82] discussed ongoing research in Finland on the use of information and communication technologies (ICT) for addressing the challenges offered by an increasing number of the aging population. They propose that the older population needs assistance not only within the boundaries of their homes but also while moving as active members of an information society. They identify the security, privacy, financial costs, usability, user involvement, and missing advanced technologies needed for designing effective solutions as the main related challenges.

Hofmann [83] reviewed ethical challenges offered by welfare technologies, i.e., the technologies for tracking, disease monitoring, as well as technology for distance treatment. A large part of AAL solutions constitutes welfare technologies. They submit that the privacy risks and disadvantages of these technologies can be challenging to balance against their potential benefits. Zagler et al. [84] proposed that privacy was one of the critical issues in AAL spaces. They proposed the use of non-invasive sensors, keeping the data within the boundaries of a smart home hosting older adults, offering complete transparency, and enabling users to suspend any service or function, if they wanted, for enhanced privacy protection.

Caire et al. [9] investigated the privacy challenges in AAL systems. They propose that a combination of the general-purpose privacy protection techniques such as encryption and granting users control over their data in AML spaces can be a possible solution to privacy problems in AAL spaces. However, they forget the lack of competence and cognitive issues of such users to accomplish this complex task [19,24]. Thorstensen [10] discussed the impact of AAL technologies on the requirement of free consent, a primary condition for privacy self-management. They argue that there is a conflict between the advantages of AAL systems and the requirements of privacy, such as informed consent. They propose that one of the solutions to solving this problem is by reducing the number of choices needed to be made by the users of smart systems living in AAL spaces.

Psychoula et al. [69] proposed a framework for privacy modeling computation and management for AAL systems within Smart Homes. They developed a metric to compute the sensitivity of the information collected in AAL spaces and suggested that it could be used for access control and recommendation of privacy settings. They computed their metric using information items, number of users accessing the information item, weight of information item’s sensitivity, the user of the smart environment, and willingness of a user to release the information item.

9.2. Privacy Settings of Android Apps

Privacy settings of Android Apps and related issues have been the focus of numerous recent researches. Tschersich [85] investigated how restrictive default privacy settings influenced user behavior on social networking sites and how different privacy settings affected their privacy management practices. They found that different users had different configuration behaviors, and non-user friendly design of privacy configuring tools kept users from effective privacy management. Alqarni and Sampalli [31] proposed a conceptual model called the ’Privacy Settings Model’ for helping social networking sites (SNS) users to understand, control, and update their privacy settings. Their model aims to assist users when choosing privacy settings of SNS and to inform them of

existing and updated privacy settings regularly. Hossain and Zhang [33] conducted a user study to learn about user views of online privacy, user knowledge about privacy settings of social apps, and user awareness of privacy disclosure. They found that 44% of the participants of their study lacked the knowledge about privacy policies and mechanisms of their OSNs; 34% of the participants showed severe concerns about their privacy protection, and 80% of the participants thought that online social networks offered inadequate privacy setting options.

Dogruel et al. [29] examined the impact of default privacy settings and expert recommendations on smartphone users' willingness to pay for "privacy-enhanced" 'features of paid applications. They found that Android users who had installed paid apps on their smartphones and had more significant privacy concerns were ready to pay for privacy premium features to ensure their privacy protection whether or not experts recommended the settings. Watson et al. [30] studied users' privacy attitudes and information disclosure preferences to find that community data could be used to create privacy settings that could better match users' privacy expectations. Lin et al. [27] proposed that automated tools used for behavioral analysis of mobile apps could not assess people perceptions during privacy decisions. They showed that crowdsourcing was a better way to record users' privacy expectations and used custom interfaces to warn users about privacy settings of apps. Nakamura et al. [28] proposed a machine learning-based approach combining prediction and clustering for predicting privacy preferences by generating privacy profiles based on data collected from users. They trained their system on data collected data from 10,000 users. Their system can generate privacy settings by asking privacy related questions from users and using historical data.

Taylor and Martinovic [70] proposed a contextual permission analysis framework and implemented it as a tool called SecuRank. SecuRank allows users to audit their installed apps and recommends whether any of the installed apps can be replaced by a functionally similar app requiring fewer data and critical device resources for its functions. They also recommend use of nudges to warn users regarding permissive default settings. However, this may adversely affect the user experience and users may ignore such warnings due to their ignorance [70]. Similarly, some researchers suggest 'individualization' of privacy settings [86], however, when it is known that a large majority of users are privacy-ignorant, such individualization will only lead to privacy-adverse settings based upon previous adverse settings. Torre et al. [32] proposed a framework for assisting user in taking informed decisions. They developed a Personal Data Manager (PDM) and an Adaptive Inference Discovery Service (AID-S). In their framework, PDM manages all data related to the user and AID-S computes the risk of possible inference of user information.

Elahi and Wang [47] proposed a participatory approach for determining the default App settings. They proposed using the skills of expert users for determining the default privacy settings of Android Apps. However, the default settings problem does not exist after Android 6.0.

9.3. Soft Sets and MCDM

Maji et al. [87] proposed that soft sets had an inherent advantage over conventional mathematical applications in MCDM problems. They explained that contrary to the conventional mathematical models soft sets did not need 'exact solutions' and could effectively handle approximate inputs. Roy and Maji [41] suggested that recently proposed theories like the theory of probability, fuzzy set theory, intuitionistic fuzzy sets, vague sets, the theory of interval mathematics, rough set theory, etc. used for dealing with uncertain and imprecise data suffered from the limitation of the inability to handle parameterization. They suggested that soft sets were a better tool for solving problems involving parameterized input.

In recent years, soft sets have been used in different problems including MCDM. Tiwari et al. [88] used a soft sets based approach in design concept evaluation. Their approach used soft sets for handling different design criteria of the designers and the preferences of the customers. In a later work, Tiwari et al. [89] integrated soft sets, Shannon's Entropy and the Technique for Order of Preference by Similarity, to Ideal Solution to propose a different approach for solving the problem of design concept evaluation. Again, soft sets were the tool to define the attributes of an object through approximate descriptions of the design criteria and linguistic requirements of customers. Ma et al. [54] surveyed recently proposed soft set based methods proposed to solve decision-making problems. They proposed that soft set based approaches were a strong candidate for designing solutions involving uncertainty and decision making.

It is evident from the literature review that although many works identify privacy as a significant issue in AAL spaces in the smart cities, there are very few works on specific privacy issues. Notably, the privacy issues arising due to the gap among the competence of elderly App users in smart cities and the privacy management requirements of Android Apps in AAL spaces and related problems are under-researched. Likewise, the research on the management of privacy settings of Android Apps ignores AAL apps and AAL users. Moreover, despite their advantages in solving MCDM problems, soft sets have not been used in the privacy-related decision-making problems.

10. Conclusion

Smart cities are facing different challenges due to an increase in the aging population. AAL systems, building on AI and ML techniques, can help in dealing with these pressing challenges. However, their users have special needs. The design, development, and deployment of AAL systems should reflect consideration of these needs. While some of these needs, such as additional care requirements, get addressed frequently, others, such as their inability to self-manage privacy due to cognitive impairments and related issues, are ignored. In this paper, we focussed on the privacy protection of the elderly Android App users while reducing their cognitive loads resulting from the complex decision-making requirements of privacy self-management. We followed an HCAI-inspired approach that integrated privacy as a shared responsibility model. We engaged Android expert users and learned their privacy decisions and preferences and used them as a reference for improving the privacy protections of the elderly Android users in smart cities. We used soft sets to model and evaluate the preferences and decisions of expert users. We proposed two algorithms, PPPA-I and PPPA-II, for determining optimal privacy settings of an AAL App and handling runtime Permission requests. The proposed approach and algorithms can improve the privacy protection of older Android users in smart cities and achieve cognitive offloading by removing user-interaction requirements.

CRediT authorship contribution statement

Haroon Elahi: Conceptualization, Methodology, Data curation, Formal analysis, Writing - original draft, Investigation. **Aniello Castiglione:** Writing - review & editing, Validation. **Guojun Wang:** Supervision, Funding acquisition, Writing - review & editing. **Oana Geman:** Writing - review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work is supported in part by the National Natural Science Foundation of China under 61632009 & 61872097, in part by the Guangdong Provincial Natural Science Foundation under Grant 2017A030308006 and High-Level Talents Program of Higher Education in Guangdong Province under Grant 2016ZJ01.

Appendix A. Anonymized App Description and Permissions as Retrieved from the Play Store

A.1. Instructions

Please read the following App description and look at the list of Permissions in Table A.7. For each Permission, please mark if it is needed to be 'always allowed' for the given App functions or not. If yes, please mark the level of its necessity on a scale from 'very low' need to 'very high' need.

A.2. Anonymized App Description

Keeping up with friends is faster and easier than ever with the this app! Use it as a friends app to connect and keep up with your

Table A.7
Permissions and Respective Need Level Options.

retrieve running apps					
Needed	(a) Yes	(b) No			
Need Level	1	2	3	4	5
find accounts on the device					
Needed	(a) Yes	(b) No			
Need Level	1	2	3	4	5
add or remove accounts					
Needed	(a) Yes	(b) No			
Need Level	1	2	3	4	5
read your own contact card					
Needed	(a) Yes	(b) No			
Need Level	1	2	3	4	5
read calendar events plus confidential information					
Needed	(a) Yes	(b) No			
Need Level	1	2	3	4	5
add or modify calendar events and send emails to guests without owners' knowledge					
Needed	(a) Yes	(b) No			
Need Level	1	2	3	4	5
read your contacts					
Needed	(a) Yes	(b) No			
Need Level	1	2	3	4	5
modify your contacts					
Needed	(a) Yes	(b) No			
Need Level	1	2	3	4	5
approximate location (network-based)					
Needed	(a) Yes	(b) No			
Need Level	1	2	3	4	5
precise location (GPS and network-based)					
Needed	(a) Yes	(b) No			
Need Level	1	2	3	4	5
read your text messages (SMS or MMS)					
Needed	(a) Yes	(b) No			
Need Level	1	2	3	4	5
directly call phone numbers					
Needed	(a) Yes	(b) No			
Need Level	1	2	3	4	5
read call log					
Needed	(a) Yes	(b) No			
Need Level	1	2	3	4	5
read phone status and identity					
Needed	(a) Yes	(b) No			
Need Level	1	2	3	4	5
read the contents of your USB storage					
Needed	(a) Yes	(b) No			
Need Level	1	2	3	4	5
Modify or delete the contents of your USB storage					
Needed	(a) Yes	(b) No			
Need Level	1	2	3	4	5
take pictures and videos					
Needed	(a) Yes	(b) No			
Need Level	1	2	3	4	5
Record audio					
Needed	(a) Yes	(b) No			
Need Level	1	2	3	4	5
view Wi-Fi connections					
Needed	(a) Yes	(b) No			
Need Level	1	2	3	4	5

social network. The app is small, allowing you to save space on your phone and use social network services in 2G conditions. Many of the classic features of our full scale app are available on the app, such as sharing to a Timeline, liking photos, searching for people, and editing your profile and groups. Specific features include:

1. Find friends and family
2. Post status updates & use Facebook emoji to help relay what's going on in your world
3. Share photos and your favorite memes
4. Get notified when friends like and comment on your posts
5. Find local social events, RSVP, and make plans to meet up with friends
6. Interact with your friends by adding your own comments or reactions to their posts
7. Save photos by adding them to photo albums
8. Follow people to get their latest news
9. Look up local businesses to see reviews, operation hours, and pictures

This app does more than help you stay connected with your friends and interests. It's also your personal organizer for storing, saving and sharing photos. It's easy to share photos straight from your Android camera, and you have full control over your photos and privacy settings. You can choose when to keep individual photos private or even set up a secret photo album to control who sees it.

It also helps you keep up with the latest news and current events around the world. Subscribe to your favorite celebrities, brands, websites, artists, or sports teams to follow their News Feeds from the convenience of your app!.

A.3. Permissions and Respective Need Level Options

In need levels, 1 = Very low, 2 = Low, 3 = Medium, 4 = High and 5 = Very high.

References

[1] UNDESA, World population prospects 2019: Highlights, Tech. Rep. ST/ESA/SER. A/423, United Nations, Department of Economic and Social Affairs, Population Division (Jun 2019)..

[2] J. Esch, A survey on ambient intelligence in healthcare, Proc. IEEE 101 (12) (2013) 2467–2469.

[3] D. Giacalone, K. Wendin, S. Kremer, M.B. Frøst, W.L. Bredie, V. Olsson, M.H. Otto, S. Skjoldborg, U. Lindberg, E. Risvik, Health and quality of life in an aging population – food and beyond, Food Qual. Prefer. 47 (2016) 166–170.

[4] A.A.K. Miller, Smart-home technologies to assist older people to live well at home, J. Aging Sci. 01 (01) (2013) 1–9.

[5] C. Dobbins, R. Rawassizadeh, E. Momeni, Detecting physical activity within lifelogs towards preventing obesity and aiding ambient assisted living, Neurocomputing 230 (2017) 110–132.

[6] D. Betti, L. Rossi, V. Stara, E. Tecchio, G. Zanella, M. Zancanaro, Assisted coaching for older people: Initial considerations, in: Lecture Notes in Electrical Engineering, Springer International Publishing, 2019, pp. 341–352.

[7] J.O. van Heek, E.-M. Schomakers, M. Ziefle, Bare necessities? how the need for care modulates the acceptance of ambient assisted living technologies, Int. J. Med. Informatics 127 (2019) 147–156.

[8] X. Zhou, K. Li, G. Xiao, Y. Zhou, K. Li, Top k favorite probabilistic products queries, IEEE Trans. Knowl. Data Eng. 28 (10) (2016) 2808–2821.

[9] P. Caire, A. Moawad, V. Efthymiou, A. Bikakis, Y. Le Traon, Privacy Challenges in Ambient Intelligence Systems, J. Ambient Intelligence Smart Environ. 8 (6) (2016) 619–644.

[10] E. Thorstensen, Privacy and future consent in smart homes as assisted living technologies, in: Human Aspects of IT for the Aged Population. Applications in Health, Assistance, and Entertainment, Springer International Publishing, 2018, pp. 415–433..

[11] J. Hao, A. Bouzouane, S. Gaboury, Recognizing multi-resident activities in non-intrusive sensor-based smart homes by formal concept analysis, Neurocomputing 318 (2018) 75–89.

[12] A.K. Sangaiah, D.V. Medhane, T. Han, M.S. Hossain, G. Muhammad, Enforcing position-based confidentiality with machine learning paradigm through mobile edge computing in real-time industrial informatics, IEEE Trans. Industr. Inf. 15 (7) (2019) 4189–4196.

[13] D. P. Ong, E. J. L. S. Pedro, M. E. M. Valenzuela, N. M. C. Tiglao, BrainSmart: Ambient assisted living system smartphone app prototype for parkinson's disease patients, in: 2018 IEEE Global Humanitarian Technology Conference (GHTC), IEEE, 2018, pp. 1–6..

[14] J.P. Pienaar, R.M. Fisher, G.P. Hancke, Smartphone: The key to your connected smart home, in: 2015 IEEE 13th International Conference on Industrial Informatics (INDIN), IEEE, 2015, pp. 999–1004.

[15] A.E. Murabet, A. Abtoy, A. Touhafi, A. Tahiri, Ambient assisted living system's models and architectures: A survey of the state of the art, J. King Saud University – Computer Inform. Sci. 32 (1) (2020) 1–10.

[16] A. Sami, W. Jenny, B. George, B. Rachelle, Privacy and the internet of things (iot) monitoring solutions for older adults: A review, in: Studies in Health Technology and Informatics 252 (Connecting the System to Enhance the Practitioner and Consumer Experience in Healthcare), 2018, pp. 8–14.

[17] S. Zhang, G. Wang, M.Z.A. Bhuiyan, Q. Liu, A dual privacy preserving scheme in continuous location-based services, IEEE Internet Things J. 5 (5) (2018) 4191–4200.

[18] M.C. Costello, E.K. Bloesch, Are older adults less embodied? a review of age effects through the lens of embodied cognition, Front. Psychol. 8 (2017) 1–18.

[19] R. Frey, R. Mata, R. Hertwig, The role of cognitive abilities in decisions from experience: Age differences emerge as a function of choice set size, Cognition 142 (2015) 60–80.

[20] D.J. Solove, Privacy Self-Management and the Consent Dilemma, 126, Harvard Law Review 1880 (2013) 1880–1903.

[21] H. Elahi, G. Wang, T. Peng, J. Chen, AI and its risks in android smartphones: A case of google smart assistant, in: Communications in Computer and Information Science, Springer Singapore, 2019, pp. 341–355.

[22] D. Vecchiato, M. Vieira, E. Martins, The perils of android security configuration, Computer 49 (6) (2016) 15–21.

[23] H. Elahi, G. Wang, J. Chen, Pleasure or pain? an evaluation of the costs and utilities of bloatware applications in android smartphones, J. Network Computer Appl. 157 (2020) 102578.

[24] G. López, G. Marín, M. Calderón, Characterizing ubiquitous systems privacy issues by gender and age, in: Lecture Notes in Computer Science, Springer International Publishing, 2015, pp. 247–258.

[25] A. Castiglione, R. De Prisco, A. De Santis, Do You Trust Your Phone?, in: T. Di Noia, F. Buccafurri (Eds.), E-Commerce and Web Technologies, Springer, Berlin Heidelberg, Berlin, Heidelberg, 2009, pp. 50–61.

[26] J. Sweller, P. Ayres, S. Kalyuga, Intrinsic and extraneous cognitive load, in: Cognitive Load Theory, Springer, New York, 2011, pp. 57–69.

[27] J. Lin, N. Sadeh, S. Amini, J. Lindqvist, J. I. Hong, J. Zhang, Expectation and purpose, in: Proceedings of the 2012 ACM Conference on Ubiquitous Computing - UbiComp '12, ACM Press, 2012, pp. 501–510..

[28] T. Nakamura, S. Kiyomoto, W.B. Tesfay, J. Serna, Easing the burden of setting privacy preferences: A machine learning approach, in: Communications in Computer and Information Science, Springer International Publishing, 2017, pp. 44–63.

[29] L. Dogruel, S. Joeckel, J. Vitak, The valuation of privacy premium features for smartphone apps: The influence of defaults and expert recommendations, Comput. Hum. Behav. 77 (2017) 230–239.

[30] J. Watson, H.R. Lipford, A. Besmer, Mapping user preference to privacy default settings, ACM Trans. Computer-Human Interaction 22 (6) (2015) 1–20.

[31] A. Alqarni, S. Sampalli, Privacy-enhancing of user's behaviour toward privacy settings in social networking sites, in: Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems - CHI EA '16, ACM Press, 2016, pp. 2758–2765..

[32] I. Torre, O.R. Sanchez, F. Koceva, G. Adorni, Supporting users to take informed decisions on privacy settings of personal devices, Pers. Ubiquit. Comput. 22 (2) (2017) 345–364.

[33] A.A. Hossain, W. Zhang, Privacy and security concern of online social networks from user perspective, in: ICISSP 2015 - International Conference on Information Systems Security and Privacy, Proceedings, IEEE, Angers, France, 2015, pp. 246–253..

[34] M.O. Riedl, Human-centered artificial intelligence and machine learning, Human Behavior Emerging Technol. 1 (1) (2019) 33–36.

[35] P. Maji, A. Roy, R. Biswas, An application of soft sets in a decision making problem, Computers Math. Appl. 44 (8–9) (2002) 1077–1083.

[36] T.-C. Wang, H.-D. Lee, Developing a fuzzy TOPSIS approach based on subjective weights and objective weights, Expert Syst. Appl. 36 (5) (2009) 8980–8985.

[37] K. Hayat, M.I. Ali, F. Karaaslan, B.-Y. Cao, M.H. Shah, Design concept evaluation using soft sets based on acceptable and satisfactory levels: an integrated TOPSIS and shannon entropy, Soft. Comput. 2020 (24) (2019) 2229–2263.

[38] D. Molodtsov, Soft set theory—first results, Computers Math. Appl. 37 (4–5) (1999) 19–31.

[39] B. Azvine, W. Wobcke, Human-centred intelligent systems and soft computing, BT Technol. J 16 (3) (1998) 125–133.

[40] ALRC, Serious Invasions of Privacy in the Digital Era, Tech. Rep. 3 September, Australian Law Reform Commission, Sydney NSW 2001 (2014). https://tinyurl.com/t3mrrcm..

[41] A. Roy, P. Maji, A fuzzy soft set theoretic approach to decision making problems, J. Comput. Appl. Math. 203 (2) (2007) 412–418.

[42] P. Maji, R. Biswas, A. Roy, Soft set theory, Computers Math. Appl. 45 (4–5) (2003) 555–562.

[43] A.Z. Khameneh, A. Kılıçman, Multi-attribute decision-making based on soft set theory: A systematic review, Soft. Comput. 23 (16) (2018) 6899–6920.

[44] Y. Yao, Relational interpretations of neighborhood operators and rough set approximation operators, Inf. Sci. 111 (1–4) (1998) 239–259.
[45] T. Lin, Granular computing on binary relations II: rough set representations and belief functions, Rough Sets Knowl. Discovery 1 (1998) 121–140.
[46] G. Dwivedi, R.K. Srivastava, S.K. Srivastava, A generalised fuzzy TOPSIS with improved closeness coefficient, Expert Syst. Appl. 96 (2018) 185–195.
[47] H. Elahi, G. Wang, A participatory privacy protection framework for smartphone application default settings, in: Communications in Computer and Information Science, Springer Singapore, 2019, pp. 168–182.
[48] E.F. Risko, S.J. Gilbert, Cognitive offloading, Trends Cognitive Sci. 20 (9) (2016) 676–688.
[49] S. Amershi, M. Cakmak, W.B. Knox, T. Kulesza, Power to the people: The role of humans in interactive machine learning, AI Magazine 35 (4) (2014) 105–120.
[50] C. Chesta, L. Corcella, S. Kroll, M. Manca, J. Nuss, F. Paternò, C. Santoro, Enabling personalisation of remote elderly assistant applications, in: Proceedings of the 12th Biannual Conference on Italian SIGCHI Chapter - CHItaly '17, ACM Press, 2017, pp. 1–9..
[51] M. Pascalev, Privacy exchanges: restoring consent in privacy self-management, Ethics Inf. Technol. 19 (1) (2016) 39–48.
[52] A.S. Billis, E.I. Papageorgiou, C.A. Frantzidis, M.S. Tsatali, A.C. Tsolaki, P.D. Bamidis, A decision-support framework for promoting independent living and ageing well, IEEE J. Biomed. Health Inform. 19 (1) (2015) 199–209.
[53] Y. Chen, K. Li, W. Yang, G. Xiao, X. Xie, T. Li, Performance-aware model for sparse matrix-matrix multiplication on the sunway taihulight supercomputer, IEEE Trans. Parallel Distrib. Syst. 30 (4) (2019) 923–938.
[54] X. Ma, Q. Liu, J. Zhan, A survey of decision making methods based on certain hybrid soft set models, Artif. Intell. Rev. 47 (4) (2016) 507–530.
[55] P. Zave, M. Jackson, E. Gunter, C. Gunter, A reference model for requirements and specifications, IEEE Softw. 17 (3) (2000) 37–43.
[56] M.H. Mobasheri, D. King, M. Johnston, S. Gautama, S. Purkayastha, A. Darzi, The ownership and clinical use of smartphones by doctors and nurses in the UK: a multicentre survey study, BMJ Innovations 1 (4) (2015) 174–181.
[57] Y. Liu, X. Liu, Fuzzy Soft Set Multi-Attribute Decision Making Method Based on TOPSIS with Improved Entropy Weight, in: Z. Tan, J. Shi, J. Wu (Eds.), Proceedings of the 2018 International Conference on Network, Communication, Computer Engineering (NCCE 2018), Vol. 147, Atlantis Press, Chongqing, 2018, pp. 321–332..
[58] H. Elahi, G. Wang, D. Xie, Assessing privacy behaviors of smartphone users in the context of data over-collection problem: An exploratory study, in: 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), IEEE, 2017, pp. 1–8..
[59] M. Hassan, A. Malik, D. Fofi, B. Karasfi, F. Meriaudeau, Towards health monitoring using remote heart rate measurement using digital camera: A feasibility study, Measurement 149 (2020) 106804.
[60] H. Elahi, G. Wang, X. Li, Smartphone bloatware: An overlooked privacy problem, in: Security, Privacy, and Anonymity in Computation, Communication, and Storage, Springer International Publishing, 2017, pp. 169–185.
[61] E. Alepis, C. Patsakis, Trapped by the UI: The android case, in: Research in Attacks, Intrusions, and Defenses, Springer International Publishing, 2017, pp. 334–354..
[62] D. Vecchiato, M. Vieira, E. Martins, A security configuration assessment for android devices, in: Proceedings of the 30th Annual ACM Symposium on Applied Computing - SAC '15, ACM Press, 2015, pp. 2299–2304..
[63] F. Parker, J. Ophoff, J.-P.V. Belle, R. Karia, Security awareness and adoption of security controls by smartphone users, in: 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec), IEEE, 2015, pp. 99–104.
[64] C. Chen, K. Li, A. Ouyang, Z. Tang, K. Li, Gpu-accelerated parallel hierarchical extreme learning machine on flink for big data, IEEE Trans. Syst. Man Cybern. Syst. 47 (10) (2017) 2740–2753.
[65] Y. Xu, G. Wang, J. Ren, Y. Zhang, An adaptive and configurable protection framework against android privilege escalation threats, Future Generation Computer Systems 92 (2019) 210–224.
[66] C.L. Oguego, J.C. Augusto, A. Muñoz, M. Springett, A survey on managing users' preferences in ambient intelligence, Univ. Access Inf. Soc. 17 (1) (2017) 97–114.
[67] S. Mitra, Y. Hayashi, Bioinformatics with soft computing, IEEE Trans. Syst., Man Cybern., Part C (Appl. Reviews) 36 (5) (2006) 616–635.
[68] C. Chen, K. Li, A. Ouyang, K. Li, Flinkcl: An opencl-based in-memory computing architecture on heterogeneous CPU-GPU clusters for big data, IEEE Trans. Computers 67 (12) (2018) 1765–1779.
[69] I. Psychoula, L. Chen, F. Chen, Privacy modelling and management for assisted living within smart homes, in: 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), IEEE, 2017, pp. 1–6..
[70] V. F. Taylor, I. Martinovic, SecuRank, in: Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices - SPSM'16, ACM Press, 2016, pp. 168–182..
[71] C. Chen, K. Li, A. Ouyang, Z. Zeng, K. Li, Gflink: An in-memory computing architecture on heterogeneous CPU-GPU clusters for big data, IEEE Trans. Parallel Distrib. Syst. 29 (6) (2018) 1275–1288.
[72] F. Palmieri, U. Fiore, A. Castiglione, Automatic security assessment for next generation wireless mobile networks, Mobile Inform. Syst. 7 (3) (2011) 217–239.
[73] The European Parliament and the Council of the European Union, Regulation (EU) 2016/679 (GDPR), Official Journal of the European Union L 119 (2016) 1–88..
[74] J. Lahtiranta, S. Hyrynsalmi, J. Koskinen, The false prometheus, ACM SIGCAS Computers and Society 47 (3) (2017) 86–97.
[75] J. Carneiro, P. Saraiva, L. Conceição, R. Santos, G. Marreiros, P. Novais, Predicting satisfaction: Perceived decision quality by decision-makers in web-based group decision support systems, Neurocomputing 338 (2019) 399–417.
[76] Y. Xu, W. Gao, Q. Zeng, G. Wang, J. Ren, Y. Zhang, A feasible fuzzy-extended attribute-based access control technique, Security and Communication Networks 2018 (2018) 1–11.
[77] G. Carullo, A. Castiglione, G. Cattaneo, A. D. Santis, U. Fiore, F. Palmieri, FeelTrust: Providing trustworthy communications in ubiquitous mobile environment, in: 2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA), IEEE, 2013..
[78] T.-R. Chang, E. Kaasinen, K. Kaipainen, Persuasive design in mobile applications for mental well-being: Multidisciplinary expert review, Social Informatics and Telecommunications Engineering, Springer, Berlin Heidelberg, 2013, pp. 154–162.
[79] A. Pal, F.M. Harper, J.A. Konstan, Exploring question selection bias to identify experts and potential experts in community question answering, ACM Trans. Inform. Syst. 30 (2) (2012) 1–28.
[80] M. Dee, V.L. Hanson, A pool of representative users for accessibility research, ACM Trans. Accessible Computing 8 (1) (2016) 1–31.
[81] A.R. Senarath, N.A.G. Arachchilage, Understanding user privacy expectations: A software developer's perspective, Telematics Inform. 35 (7) (2018) 1845–1862.
[82] K.E. Skouby, A. Kivimäki, L. Haukipuro, P. Lynggaard, I. Windekilde, Smart Cities and the Ageing Population, Wireless World Research Forum 12 (2014) 1–12.
[83] B. Hofmann, Ethical challenges with welfare technology: A review of the literature, Sci. Eng. Ethics 19 (2) (2012) 389–406.
[84] W. L. Zagler, P. Panek, M. Rauhala, Ambient assisted living systems - the conflicts between technology, acceptance, ethics and privacy, in: A. I. Karshmer, J. Nehmer, H. Raffler, G. Tröster (Eds.), Assisted Living Systems - Models, Architectures and Engineering Approaches, no. 07462 in Dagstuhl Seminar Proceedings, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany, Dagstuhl, Germany, 2008, pp. 1–4..
[85] M. Tschersich, Configuration behavior of restrictive default privacy settings on social network sites, in: Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance, Springer International Publishing, 2015, pp. 77–94.
[86] S. Egelman, E. Peer, The myth of the average user, in: Proceedings of the New Security Paradigms Workshop on ZZZ - NSPW '15, ACM Press, 2015, pp. 16–28..
[87] K. Gong, Z. Xiao, X. Zhang, The bijective soft set with its operations, Computers Math. Appl. 60 (8) (2010) 2270–2278.
[88] V. Tiwari, P.K. Jain, P. Tandon, Product design concept evaluation using rough sets and VIKOR method, Adv. Eng. Inform. 30 (1) (2016) 16–25.
[89] V. Tiwari, P.K. Jain, P. Tandon, An integrated shannon entropy and TOPSIS for product design concept evaluation based on bijective soft set, J. Intell. Manuf. 30 (4) (2017) 1645–1658.

Haroon Elahi is currently pursuing his doctoral degree in the School of Computer Science and Technology, Guangzhou University, China. He graduated from Blekinge Institute of Technology, Sweden in Computer Science. Before that, he studied Ubiquitous Computing at the same institute. He also earned degrees in IT and Commerce from Pakistan. Before beginning his Ph.D. studies in China, he was working as an Assistant Professor at the University of South Asia in Pakistan. He has also worked with professional-trainings, project design, product design, and software development. The focus of his current research is the state of privacy and security in smartphone devices in the rapidly changing threat landscape. He is a preacher of ubiquitous computing design methods and techniques.

Aniello Castiglione (S'04 M'08) received the Ph.D. degree in Computer Science from the University of Salerno, Italy. He is currently with the Department of Science and Technology, University of Naples Parthenope, Italy. He authored over 200 papers in international journals (14 journal papers are published on IEEE / ACM Transactions and) and conferences. His current research interests include Information Forensics, Digital Forensics, Security and Privacy on distributed systems, Communication Networks, Applied Cryptography, and Sustainable Computing.
Dr. Castiglione has served in the organization (mainly as the Program Chair and a TPC member) of more than 200 international conferences. He served as a Reviewer for approximately 100 international journals and the

Managing Editor of two ISI-ranked international journals. He was a Guest Editor of around 20 special issues and served as an Editor on more than 10 Editorial Boards of international journals. One of his papers (published in the IEEE Transactions on Dependable and Secure Computing) was selected as the "Featured Article" in the "IEEE Cybersecurity Initiative" in 2014, while in 2018 another paper (published in the IEEE Cloud Computing Magazine) was selected as the "Featured Article" in the "IEEE Cloud Computing Initiative."

Guojun Wang, received BSc in Geophysics, MSc in Computer Science, and PhD in Computer Science from Central South University, China. He is currently Pearl River Scholarship Distinguished Professor and Vice Dean of School of Computer Science and Technology at Guangzhou University, China. He is also Director of Institute of Computer Networks at Guangzhou University, China. He was Professor at Central South University, China; Visiting Scholar at Temple University and Florida Atlantic University, USA; Visiting Researcher at The University of Aizu, Japan; and Research Fellow at The Hong Kong Polytechnic University. His research interests include artificial intelligence, big data, cloud computing, and cyberspace security. He is a distinguished member of CCF, and a member of IEEE, ACM, and IEICE.

Oana Geman, received her PhD in Electronics and Telecommunication. She is currently an Associate Professor at the University of Suceava, Romania and obtained Habilitation. Her expertise includes: non-invasive measurements of biomedical signals, wireless sensors, signal processing, and processing information, Data-Mining, Deep Learning, Intelligent Systems and Biomedical Applications. Within the past five years she published 6 books, has published over 66 articles (45 articles in ISI Web of Science journals, 15 articles in ISI indexed conference volumes as main author, and 6 papers in Q1and Q2 Journals, with IF over 30), and her various works have been cited over 600 times.