Quantizing Personal Privacy in Ubiquitous Computing

Tinghuai Ma[1,2], Wei Tian[1] , Donghai Guan[3] and Sungyoung Lee[3]
[1] School of Computer & Software, Nanjing University of Information Science & Technology
Nanjing, 210044, P.R. China
[e-mail: {thma,tw}@nuist.edu.cn]
[2] Center of Network Monitoring, Jiangsu Province
Nanjing, 210044, P.R. China
[e-mail: thma@nuist.edu.cn]
[3]Department of Computer Engineering, Kyung Hee University
Gyeonggi, 446-701, Korea
[e-mail: {donghai, sylee}@oslab.khu.ac.kr]
*Corresponding author: Tinghuai Ma

Received July 24, 2011; accepted January 6, 2011;
published September 29, 2011

Abstract

Privacy is one of the most important and difficult research issues in ubiquitous computing. It is qualitative rather than quantitative. Privacy preserving mainly relies on policy based rules of the system, and users cannot adjust their privacy disclosure rules dynamically based on their wishes. To make users understand and control their privacy measurement, we present a scheme to quantize the personal privacy. We aim to configure the person's privacy based on the numerical privacy level which can be dynamically adjusted. Instead of using the traditional simple rule engine, we implement this scheme in a complex way. In addition, we design the scenario to explain the implementation of our scheme. To the best of our knowledge, we are the first to assess personal privacy numerically to achieve precision privacy computing. The privacy measurement and disclosure model will be refined in the future work.

Keywords: Ubiquitous computing, personal privacy, quantizing, disclosure, scheme

This work was supported in part by the National Science Foundation under Grant No.61173143, and also supported by A Project Funded by the Priority Academic Program Development of Jiangsu Higher Education Institutions. This research was supported by the MKE (Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Centre) support program supervised by the IITA (Institute of Information Technology Advancement)" (IITA-2009-(C1090-0902-0002)).

DOI: 10.3837/tiis.2011.09.009

1. Introduction

Ubiquitous computing represents the concept of seamless 'everywhere' computing and aims at making computing and communication essentially transparent to the users. In ubiquitous computing environment, we will be surrounded with a comfortable and convenient information environment that merges physical and computational infrastructures into an integrated habitat [1]. Context-awareness will allow this habitat to take on the responsibility of serving users, by tailoring itself to their preferences as well as performing tasks and group activities according to the nature of the physical space. So, the more an application is aware of the user's context, the better it can adapt itself to assist him. On the other hand, the more an application knows the user, the greater the threat that it will pose to user's privacy [2]. Thus, privacy in ubiquitous computing has been a contentious issue. The privacy concerns have been raised to suggest that privacy may be the greatest barrier to the long-term success of ubiquitous computing [3].

Privacy preserving in the ubiquitous computing mainly focuses on two aspects. One is the anonymous / pseudonym oriented, the other is the policy based.

For the anonymous based privacy enhancing technology, there are *k*-anonymities which can't be distinguished from each other. In other words, there are k entities having the same ID or in the same location at the same time. The higher value of *k*, the higher level of anonymity is [4]. The service provider doesn't want to misuse of data because there is a mixture of true and k-1 sensor data. Even though there are k IDs, the privacy sensitive information may be revealed to an attacker through track analysis. The combination of frequently varying pseudonyms and dummy traffic is used to prevent it [5]. For some ID based services, the virtual identities are used to conceal the user's real identity [6]. Anonym and authentication are always conflict. Nguyen Ngoc Diep presents a scheme using anonymous user ID, sensitive data sharing method, and account management to provide a lightweight authentication while keeping users anonymously interacting with the services in a secure and flexible way [7]. Qi He uses blind signature to encrypt anonymous ID, which can support the anonymous ID's authority [8].

The main concept in policy based privacy enhancing technology is storing privacy-compliant rules to process personal information. The stored privacy policies describe the allowed recipients, uses, and storage duration of users' data. Also, a policy engine is used to reason the compatible privacy policy. Now, privacy policy is described in XML [9][10] and XACML [11]. Most privacy policy based privacy enhancing technologies (PET) are focus on one or more scenarios. The configuration of policy for each scenario is a huge work [12]. The management and deducing are the main concerns in policy based system [13][14][15][16]. Policy based PET is simply, intuitive, but not easy to deploy in wide area.

The above PETs mainly focus on conventional data management schemes to support user privacy preserving. Although the privacy does not always need to preserve, sometimes it is important when sharing information with others. Let us consider the scenario that we preserve the students' blood type and allergies in campus and share them for prompt treatment in emergency. It is dynamic that the information is privacy or not. This depends on the user's environment, and the privacy level user sets. It implies that privacy depends not only on sets of rules to resolve situations, but also on the granularity of user-specific privacy levels. It is also important to estimate the user's privacy level in different scenario for deciding which information will be disclosed. This makes it necessary for us to measure the privacy level.

In this paper, we present a scheme for quantizing user privacy according to user's profile and preferences. We provide a mechanism for user to dynamically modify his privacy level for disclosing information according to the capability of the environment's privacy protected level. Our scheme aims to configure the user's privacy information disclosing level (1) based on the overall privacy set by the user and (2) dynamically, based on the user's modification of privacy policies. We discuss the motivation for our work in Section 2. Section 3 presents some of the related work in privacy and privacy measurement. We describe our proposed scheme in Section 4 and analyze it in Section 5. At last, we conclude the paper in Section 6.

2. Motivation

The privacy enhancing technology (PET) requires the user to abide the policy rule that system has set. There is no way for users to modify or change the rules and policies. So, if the user preferences and the service provider policy do not match, the only option for the user giving up this service. This provides nothing more than a simple "take it or leave it" dualism [17] (Maaser *et al*., 2006). For success of the deal, users have to give up more privacy than what they would prefer; otherwise, they will be excluded from using interesting services. The service providers may lose some concerned users while keeping their critical privacy policies, which against the user requirement to protect their privacy.

It is necessary to permit users to modify their privacy level for right privacy information disclosing. Especially in a significant scale, it's a challenge to deploy ubiquitous computing services for making adequate provision for handling personal privacy. It's a terrible work to design a ubiquitous middleware to encompass the myriad information flows into rule sets and incorporate them. The key solution is to design a framework which can adapt to a highly dynamic environment based on existing privacy policy. To illustrate this problem, we present the following scenario:

John logs into a recommend system for reviewing the house sales information. There are three house- agencies A, B, C in the system. John chooses the A agency's service. He sets his privacy level high. He only allow agency A to know his name. He stores his address, and contact details as private information and make they unknown to agency A.

After that, John wants to view other information from other agencies. He finds a higher credit agency C, which has higher capability of privacy protection. During the recommend process, John set his privacy level lower to medium so that address, telephone and email are shared with agency C.

In the above scenario, John's profile has been classed to different privacy levels. The privacy level changing leads to some profile information sharing or hiding, as john's address and contact information changed the role from hiding to public. But here it is rule based to control what and when the role should change. The rules are the predefined privacy policies, which are based on the social and behavioral nature of the user. The rules' enumeration is unpractical for flexibility of ubiquitous computing system. For this reason, designers are constantly involved in huge configuration steps for incorporating privacy into the system.

Further more, the existed privacy rule needs modification based upon various conditions such as location, device properties, type of user as well as the social interaction of the users. The ubiquitous system should become aware of entity's privacy level and allow the user to set his privacy levels.

The solution of these problems is to quantize the privacy information, and configure the rule sets in an automatic way. In this paper, we present a scheme for quantizing personal privacy from profile and preferences, this is the first step to realize the privacy rule sets auto configuration.

3. Related Work

In order to quantize the personal privacy, firstly, it is necessary to examine the essence of personal privacy. In this section, we survey privacy and privacy measurement in ubiquitous computing environments.

3.1 Privacy

What is the definition of privacy? In 1890s, privacy has been considered to be largely synonymous with a right to be let alone. While in 1967s, the informational privacy was defined as an individual's right to determine how, when, and to what extent information about the self will be released to another person or to an organization. In 1997s, DeCew identified expressive privacy, which "protects a realm for expressing ones self-identity or personhood through speech or activity. It protects the ability to decide to continue or to modify ones behavior when the activity in question helps define oneself as a person, shielded from interference, pressure and coercion from government or from other individuals" [18]. The national standard of Canadian Standards Association's model code for the protection of personal information, includes ten privacy principles, is be considered as representative of principles behind privacy legislation in many countries [13].

Clearly, privacy is a social, ethical and legal issue, beyond technical threats. Protecting the privacy of users is of central importance in the Ubiquitous Computing environment. The content of personal privacy in ubiquitous computing is the basic problem for privacy preserving. Tentori, M. *et al*. describe the privacy as five contextual elements: location, identity, access, activity and persistence [2]. Patrikakis, C. and Karamolegkos, P. use the user's environment, situation, preference, and status to describe personal privacy [19]. In a network circumstance, Ozturk divides the privacy into three parts: content privacy data, identity privacy data, and location privacy data [20]. Buchanan *et al*. do three investigates in order to find out what online privacies the users are concerns about [18]. The result shows that the highly concerned items include identity, medical records, online activities, credit card, email, internet address etc. Tinghuai Ma et al discuss the context in a smart home, which can be used to describe the personal preference [21]. Blaine et al classify the private data into static, dynamic, and derived data, which follow the Corby's view [22][23].

By combining the above privacy expression, we know the personal privacy information includes personal profile and the context. As shown in Table 1, we classify the personal privacy into three levels: privacy, information, and elements.

As Table 1 shows, UbiComp Sightings, mainly including timestamp and location, belong to context. Timestamp can be further divided into real-time and historical record. Real-time means timestamp is 'now' and is expressed as form as second, minute, hour, day, week, month, season seven granularities. The historical data are event occurring sequences, which can be used to record user trace. In the first phase, smart home is considered. So, the location includes bedroom, bathroom, kitchen, dining room, living room choice. Only three types of activities are considered: leaving room, staying in room, and entering room.

The person's profile is the key part of privacy. The profile is classified into four parts: Identity, background, assets, and behavior. There are several elements to describe the personal information of each part

Table 1. Personal privacy information categories

Privacy		*Information*	*Element*	*Example*
Personal Privacy	*Profile*	*Identify*	*Legal identity*	*Name, identification card, passport No., driver's License*
			Finical identity	*Bank accounts, credit card No.*
			Bio-identity	*Fingerprint, race, color, gender, height, weight, physical characteristic, retinal pattern, DNA*
			Social identity	*Membership in church, auto clubs, ethnicity*
			Digital ID	*Pseudonym, username, IP address, password*
		Background	*Relationship*	*Child, parent, spouse*
			Education	*University, major, graduate Time*
			Career	*Company, salary, occupation*
			Address	*Phone, home address, business address, Email*
			Health	*Medical history, medical insurance, physician detail*
			Records	*Financial, travel, mobile phone records*
		Assets	*Tangible*	*Building, automobiles, boats, credit balance, stock portfolios, debt balance*
			Intangible	*Insurance polices, employee agreement*
		Behavior	*Social behavior*	*Drug use, violations of law, family traits*
			Tastes	*Desire buying items, habit*
	Context	*Context*	*Real time*	*Second, minute, hour, day, week, month, season*
			Historical	*Event occurring sequence*
			Location	*Bedroom, bathroom, kitchen, dining room, living room*
			Activity	*Leaving, staying, entering*

3.2 Privacy measurement

The information considered to be private is different according to the user's privacy concerns and the information's importance. So, measuring privacy is hard and it is even harder than security measurement. The *k*-anonymities privacy protected method is the only one method that can indicate the privacy preserving level precisely. In this method, *k* represents the privacy preserving degree (Sweeney and Latanya, 2002; Cheng et al., 2005) [4][5].

Yi Lu *et al*. assign a factor $c \in [0, 1]$ to indicate the unknown degree of transferred data in a peer-to-peer network [24]. The unknown factor c also can be considered as privacy measurement. In that paper, the operation $*$ is defined for privacy calculating as follows: $c = a * b$ is calculated as *c=max* (*a, b*), where *a*, *b* are two privacy factors. From another point, George Yee presents a method to measure the privacy protected capability of web services [25]. From Internal violations (IV) and External violations (EV), it measures how well a service provider protects privacy. The IV and EV are calculated as numerical data.

The entropy is the well known method to quantify an information source's uncertainty. Privacy is an uncertainty in some sense. Patrikakis, Karamolegkos and Gautham use entropy to measure the privacy uncertainty [12][19]. Patrikakis and Karamolegkos [19] indicate that it's difficult to identify a user's personal preferences, parameters, and whereabouts, which are considered as personal privacy. But the information source's uncertainty can be quantified by Claude Shannon's theoretical mathematical framework. Thus, in different privacy level, user's reported information can be depicted as different entropy. Gautham Pallapa considers a privacy data evaluation, where data comes from multi-sensors in ubiquitous computing, aiming at infusing privacy data into precision [26][27]. This is a good case for privacy's numerical. In these two papers, each context element is assigned a probability to calculate the weight w, where w is considered as privacy measurement. Setting threshold, the w can be classified into different privacy level. If w is classified into transparent level, it means w representing information can be shared with others. Gautham Pallapa later considers use entropy theory to combine the total w to measure the privacy of situation [12], same as Patrikakis and Karamolegkos mentioned [19].

4. The proposed scheme

In this section, we propose a privacy measuring scheme based on the user's profile and context. The privacy level depends on the information's precision and information integration. The mini granular information is element as shown in table 1. So, we first calculate the elements' privacy, then integrate elements to unit information, privacy granules.

4.1 Quantifying element

As shown in Table 1, the Personal Privacy includes two parts: context and profile. There are one and four information granules in context and profile respectively. We consider these five information granules as the basic aspects to evaluate the personal privacy. In order to calculate the five information granules, the element's privacy level should be decided first.

We use uncertainty to represent the privacy of user, noted as u. For privacy of element e_i, it is noted as $u(e_i)$. In this subsection, we present an approach to assign $u(e_i)$.

Let l be the number of privacy level. Let $L = \{0, \frac{1}{l}, \frac{2}{l}, \cdots, \frac{a}{l}, \cdots 1\}$ be the permissible privacy levels, where $a<l$.

4.1.1 Mapping between privacy level and content

For each element, we can assign it a privacy level according to the element's content. For example, if the time information only includes day (without hour, minute, and second), then the time element is not definite. And there is uncertainty in time element. In our view, the time's uncertainty is 1/3. The element's uncertainty is larger; the element's privacy weight is bigger.

For the person's context, we just simply set the privacy level number to three, $l = 3$ simply. The mappings of the content and the privacy level are shown in table 2. The element's uncertainty level is referred to [28].

Table 2. The uncertainty quantifying mapping table

Information	Uncertainty=0	Uncertainty=1/3	Uncertainty=2/3	Uncertainty=3/3
Time	second/Minute/Hour	Day/Week/Month	Season	Undisclosed
Historical	Correct sequence	List event	Incomplete event	Undisclosed
Location	Room /block	Building	municipality	Undisclosed
Status	Precise	Categorical	Busy/not busy	Undisclosed

Let $u(e_i)$ denote element uncertainty of e_i, $u(I_j)$ denote information uncertainty of I_j. The information's uncertainty $u(I_j)=\sum_i u(e_i)$, where $e_i \in I_j$.

4.1.2 Element privacy initiation

According to the mapping table of Table 2 shown, the element e_i's content is decided by system or user directly, the $u(e_i)$ can be got by searching the mapping table.

In a transaction negotiation, each element's uncertainty $u(e_i)$ should be decided to satisfy the system's requirement. It is a hard work to adjust every element's uncertainty level. The system adopts follow methods.

The system first searches the transaction log for any prior existence of the element and assigns that uncertainty to $u(e_i)$ if the record of the element is available. In the absence of any record of the element in the transaction log, the system sets a default uncertainty of $u^0(e_i)=1/l$ to the element, where $u^0(e_i)$ represents the initial uncertainty of the element e_i. If uncertainty have been specified for context elements in the rule set, the corresponding uncertainty is set as the initial uncertainty for e_i.

4.2 Quantifying information

According toTable 1, different information is generated based on the elements. Since $u(e_i)$ represents the uncertainty of e_i, the uncertainty of information $u(I_j)$ is the entropy contained by I_j and is calculated by [12][19]:

$$u(I_j)=-\sum_{i=1}^{n} u(e_i)\log u(e_i) \tag{1}$$

where, $I_j=\{e_1,e_2,\cdots,e_n\}$.

$u(I_j)$ represents the uncertainty of information and its value indicates the privacy level of the information. If $u(I_j)=0$, it means that information I_j is no uncertainty to public, and can be disclosed totally. If rule has been specified for assigning information I_j to particular privacy states $u(I_j^0)$, the uncertainty of the information $u(I_j)$ is increased (or decreased) to $u(I_j^0)$ respectively using increment (or decrement) functions.

According to system set, the privacy level number is l, the interval of privacy states is $1/l$. Let P_k denote the set of privacy k th level, $1 \le k \le l$, which means the uncertainty of information is k/l. After the calculation of $u(I_j)$, the total I_j can be classified into l sets represented by P_k, $k=0,1,2,\ldots,l$, according to it's $u(I_j)$ value. If the number of information in the k th level set is q, the P_k is expressed as follows:

$$P_k=\{I_1,I_2,\cdots I_j,\cdots I_q\} \tag{2}$$

while $u(I_j)\in[\frac{k-1}{l},\frac{k}{l})$, $j=\{1,2,\cdots q\}$.

The uncertainty of each privacy level is calculated as:

$$u(P_k) = \sum_{j=1}^{q} I_j \tag{3}$$

The total personal uncertainty is the measurement of personal provided information which can be any privacy level. It can be calculated:

$$\theta = \sum_{k=0}^{l} P_k \tag{4}$$

So,

$$\theta = \sum_{k=0}^{l} P_k = \sum_{k=0}^{l} (\sum_{j=1}^{q} u(I_j)) \tag{5}$$

Let the $u(I_j)$ is replaced by equation (1),

$$\theta = -\sum_{k=0}^{l} \sum_{j=1}^{q} \sum_{i=1}^{n} u(e_i) \log u(e_i) \tag{6}$$

Obviously, the larger θ means the less of *the* personal privacy information disclosed.

4.3 Privacy changing

From equation (2), we can get the Element-Privacy Graph (EPG) as shown in **Fig. 1**, which is similar as the Context-Privacy Graph [25]. In the EPG, we can set a rule, the privacy level under a threshold φ can be transparent to others, anyone can get the personal information as long as he requests. The transparent set $C_T = \{P_1, P_2, \cdots P_T\}$, while $\frac{T}{l} < \varphi$. As shown in **Fig. 1**, the transparent set C_T is in shadow.

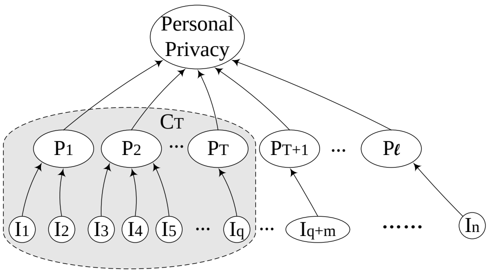


Fig. 1. A element privacy graph

4.3.1 Specific privacy level changing

Information is classified to privacy level based on their uncertainty $u(I_j)$ as shown in **Fig. 1**. As mentioned in subsection 4.2, sometimes, rule has been specified for assigning information I_j to particular privacy level P_k, the uncertainty of the information $u(I_j)$ must be increased (or decreased) to P_k. As shown in **Fig. 2**, I_1 is assigned to P_l by increasing the $u(I_1)$ to $[\frac{l-1}{l}, \frac{l}{l})$, I_{q+m} is assigned to P_T by decreasing the $u(I_{q+m})$ to $[\frac{T-1}{l}, \frac{T}{l})$.

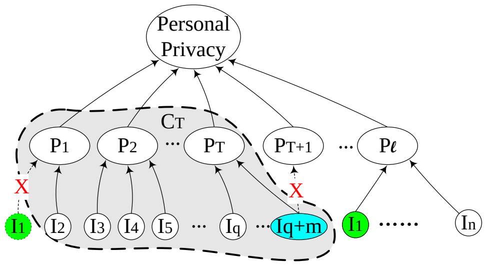


Fig. 2. A element privacy graph with specific privacy level assignment

To achieve this, Pallapa (2007a) introduces a pair of functions to increase or decrease the value of $u(I_j)$. The functions are of type [0, 1]→[0, 1], described as follows:

$$Inc_\delta(u) = \frac{(u + u^\delta)}{2} \tag{7}$$

$$Dec_\delta(u) = \frac{(u + \sqrt[\delta]{u})}{2} \tag{8}$$

Where δ is the ratio of the number of elements in information I_j to the number of total elements, where in $|I_j|$ denote the number of element in the information I_j, $\delta = \frac{|I_j|}{\sum |I_j|}$.

Assume $u(I_j)$=0.78, I_j has 5 elements, the total elements for all information is 20 elements, $\delta = \frac{5}{20}$. Now, according to some rules, the $u(I_j)$ should be at privacy level P_k, which uncertainty is 0.3. Suppose $l = 10$, according to the equation (2), while P_k's uncertainty is $\frac{k}{l} = \frac{3}{10}$, $I_j \in P_k$, so $u(I_j) \in$ $[\frac{k-1}{l}, \frac{k}{l})$ = $[0.3,0.4)$. But $Dec_\delta(u(I_j))$ = $Dec_{\frac{5}{20}}(0.78)$ = $0.575 \notin [0.3,0.4)$. So, there need multi-times to adjust the uncertainties of elements $u(e_i)$ in I_j until $u(I_j) \in [\frac{3}{10}, \frac{4}{10})$. The adjustment of $u(e_i)$ is decreased by multiples of $\frac{1}{l}$.

The uncertainties change algorithm is proposed using $Inc_\delta(u)$ and $Dec_\delta(u)$ based on Pallapa's literature [12].

As shown in algorithm of information uncertainties change in **Fig. 3**, firstly, the $Inc_\delta(u(I_j))$ or $Dec_\delta(u(I_j))$ is used to get the new $\hat{u}(I_j)$. then $u(e_i)$ is adjusted to satisfy the $\hat{u}(I_j)$ according the equation (1). This algorithm shows, there are several times to decrease / increase the $u(I_j)$ until $\hat{u}(I_j) \in [u_{\min}, u_{\max})$. In each iteration, the adjustment of $u(e_i)$ is only to satisfy the $\hat{u}(I_j)$.

```
Algorithm 1 uncertainty change
Construct EPG with $e_i, I_j, P_k$
Compare EPG with rule sets
if $I_j$ is allocated to different $P_k$ in rule set then
  Obtain uncertainty thresholds $u_{\min} = k/l$, $u_{\max} = (k+1)/l$ for proper
  privacy state $P_k$
  while( $u(I_j) < u_{\min}$ ) do
      $\hat{u}(I_j) = Inc_{\delta}(u(I_j))$
      For $e_i = e_1$ to $e_n$
          Increment $u(e_i)$ by $1/l$
          $u(I_j) = -\sum_{i=1}^{n} u(e_i)\log u(e_i)$
          if $u(I_j) > \hat{u}(I_j)$ break
      End for
  end while
  while $u(I_j) > u_{\max}$ then
      $\hat{u}(I_j) = Dec_{\delta}(u(I_j))$
      For $e_i = e_1$ to $e_n$
          decrease $u(e_i)$ by $1/l$
          $u(I_j) = -\sum_{i=1}^{n} u(e_i)\log u(e_i)$
          if $u(I_j) < \hat{u}(I_j)$ break
      End for
  end while
```

Fig. 3. algorithm of information privacy level change

4.3.2 Overall privacy level changing

As shown in scenario 2, user wants to decrease his uncertainty θ to $\hat{\theta}$ for more privacy information leakage. We note C_T as transparent set and C_P as private set. If $\hat{\theta} < \theta$, the system's uncertainty will decrease, some information in C_P will be classified into C_T. The I_j, which $u(I_j)$ is minimum has a trend to be classified into C_T. On the other hand, if $\hat{\theta} > \theta$, the system's uncertainty will increase, some information in C_T will be classified into C_P. The I_j, which $u(I_j)$ is maximum has a trend to be eliminated from C_T. From equation (4), the $u(I_j)$ will be changed for let θ to $\hat{\theta}$. The increment or decrement function is the same as function (7), (8). The algorithm is described as follows:

```
Algorithm 2 Privacy level change
sort the $u(I_j)$ in $C_T$ in Desc, and $C_P$ in Asc separately
if ( $\hat{\theta} > \theta$ )
    for $I_j$ in $C_T$
        $Inc_\delta(u(I_j))$
        For $e_i = e_1$ to $e_n$
            Increment $u(e_i)$ by $1/l$
            $u(I_j) = -\sum_{i=1}^{n} u(e_i)\log u(e_i)$
        End for
        $\theta = -\sum_{k=0}^{l}\sum_{j=1}^{q}\sum_{i=1}^{n} u(e_i)\log u(e_i)$
        if ( $\theta > \hat{\theta}$ ) break
    end for
end if
if ( $\hat{\theta} < \theta$ )
    for $I_j$ in $C_P$
        $Des_\delta(u(I_j))$
        For $e_i = e_1$ to $e_n$
            decrease $u(e_i)$ by $1/l$
            $u(I_j) = -\sum_{i=1}^{n} u(e_i)\log u(e_i)$
        End for
        $\theta = -\sum_{k=0}^{l}\sum_{j=1}^{q}\sum_{i=1}^{n} u(e_i)\log u(e_i)$
        if ( $\theta < \hat{\theta}$ ) break
    end for
end if
```

Fig. 4. algorithm of Privacy level change

Here, we provide an intuitive way for user to adjust the privacy setting of the overall system. Similar to the security level slider in the internet explorer browser of Microsoft Windows, user can assign the privacy with slider easily.

Especially, while user senses the environment's privacy protected capability, user's PDA can adjust his overall privacy setting automatically. Such as adjusting the totally uncertainty θ to a particular level, the user's PDA changes the $u(e_i)$ and $u(I_j)$ to satisfy the change of the θ. This method can also be used in negotiation between user and system.

5. Analysis

In this section, we consider the scenario presented in Section 2 and demonstrate the working of our scheme presented in the previous section. Usually, while John logs into a house recommend system, he will keep his information tightly in order to avoid boring advertisements. As mentioned above, the name will be opened to two agencies A and C, but the contact information only distributed to agency C. Assume the I_1 is identify information, I_2 is background information. I_1={legal identity, finical identity, bio-identity, social identity, digital ID}, I_2={relationship, education, career, address, Health, records }. As discussed in scenario in section 2, first John let the agency A know his name no more than others. We assume the uncertainty of elements in information I_1 , I_2 as follows:

Table 3. The initial uncertainty of each elements

	Information	*Element*	u(*Element*)
I_1	*Identify*	*Legal identity*	*0.4*
		Finical identity	*0.9*
		Bio-identity	*0.9*
		Social identity	*0.9*
		Digital ID	*0.9*
I_2	*Background*	*Relationship*	*0.9*
		Education	*0.8*
		Career	*0.7*
		Address	*0.8*
		Health	*0.7*
		Records	*0.9*

The other elements are all unknown that $u(e_i)=1$. $u(I_1)=-\sum_{i=1}^{5}u(e_i)\log u(e_i)$ =0.32, $u(I_2)=-\sum_{i=1}^{6}u(e_i)\log u(e_i)$ =0.45, θ=0.32+0.45=0.77. If John sets the threshold $\varphi=0.4$ (means the information will be disclosed if it's information uncertainty under φ). While interacts with agency A, $u(I_1)<\varphi$, so, information I_1 will be publicity. Among the information I_1 , each element's uncertainty is 0.9 except *legal identity* element. It means there is no explicit information. So, information I_1 is publicity just means the element *legal identity* will be disclosed. This is only name is disclosed in element *legal identity.*

While interacts with agency C, John adjust privacy uncertainty θ to 0.7, which is 0.77 in former. Following algorithm 2, the $u(I_2)$ should be decreased. According to equation (8), $Des_{\delta}(u(I_2))=Des_{6/11}(0.45)$ =0.34, while $\delta=\frac{\text{number of elements in information } I_2}{\text{number of total elements}}=\frac{6}{11}$. The total θ = $u(I_1)$ + $u(I_2)$ = 0.32+0.34=0.66, satisfy the final results are got as follows: $u(phone)$ =0.3, $u(address)$ =0.2, $u(email)$ = 0.1, $u(I_2)=0.3966<\varphi$, θ =0.7, after 6 times iteration for adjusting the $u(e_i)$. Thus, John discloses I_1 and I_2 .

The elements' uncertainties setting should be configured by user himself at anytime and anywhere. Of course, the system provides a default uncertainty for all the elements, then user can modify it through GUI. The system also provides a GUI to adjust the φ and $\hat{\theta}$.

Not all the time, user *must* set the parameters such as elements' uncertainties $u(e_i)$, φ , $\hat{\theta}$ and so on. The system stores the every scenario's configuration as: $T=<S_{id},\varphi,\hat{\theta},U>$, where S_{id} is the scenario session id, φ is threshold for privacy transfer, $\hat{\theta}$ is the total privacy level, $U=\{u(I_1), u(I_2), \ldots, u(I_k)\}$ for the k information of personal privacy.

6. Conclusion

It is more complex to interpret the privacy than showing a strict set of rules. How to convert the abstract nature of personal privacy into a tangible issue is the essential of privacy preserving in ubiquitous computing.

In this paper, we have presented a scheme for assessing personal privacy in ubiquitous computing. This is one part of precision privacy computing. This scheme can be extended to negotiation enhancements of privacy policies. The scheme provides an intuitive sense for user to understand their privacy measurement and control. We implement this scheme for avoiding rule engine, which is necessary in policy based privacy preserving system.

The future work includes refining the elements' uncertainty level, mapping the numerical level to the content it disclosed. More scenarios should be studied and the records form as $T=<S_{id},\varphi,\hat{\theta},U>$ are *stored*. Further more, the total quantifying of privacy preserving will be studied, including quantizing the user's credit evaluation before processing, quantizing environment privacy protected capability measurement, quantizing the risk of privacy leakage in processing. We also intend to use machine learning to predict the optimized privacy setting based on user behavior and prior interaction.

Reference

[1] M. Weiser, "The future of ubiquitous computing on campus," *Communications of the ACM*, vol. 41, no.1, pp. 41-42, 1998. Article (CrossRef Link)

[2] M. Tentori, , J. Favela, V. Gonzalez, "Quality of Privacy (QoP) for the Design of Ubiquitous Healthcare Applications," *Journal of Universal Computer Science*, vol. 12, no. 3, pp. 252-269, 2006. Article (CrossRef Link)

[3] J.I. Hong, J.D. Ng, S. Lederer, J.A. Landay, "Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems," in *Proc. of ACM conference on Designing Interactive Systems (DIS2004)*, pp.91-100, 2004. Article (CrossRef Link)

[4] L. Sweeney, "k-Anonymity: a model for protecting privacy," *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, vol.10, no.5, pp.557-570, 2002. Article (CrossRef Link)

[5] H.S. Cheng, D. Zhang, J.G. Tan, "Protection of privacy in pervasive computing environments," in *Proc. of International Conference on Information Technology: Coding and Computing(ITCC 2005)*, vol. 2, pp. 242-247, 2005.

[6] E. Papadopoulou, S. McBurney, N. Taylor, M.H. Williams, K. Dolinar, M. Neubauer, "Using User Preferences to Enhance Privacy in Pervasive Systems," in *Proc. of Third International Conference on Systems(ICONS 08)*, pp. 271-276, 2008.

[7] N.N. Diep, S. Lee, Y.-K. Lee, H.J. Lee, "A Privacy Preserving Access Control Scheme using Anonymous Identification for Ubiquitous Environments," in *Proc. of the 13th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications*, pp. 482-487, 2007.

[8] Qi He, D. Wu, P. Khosla, "The quest for personal control over mobile location privacy," *IEEE Communications Magazine*, vol. 42, no. 5, pp. 130-136, 2004. Article (CrossRef Link)

[9] M. Langheinrich, "A Privacy Awareness System for Ubiquitous Computing Environments," in *Proc. of the 4th International Conference on Ubiquitous Computing*, pp. 237–245, 2002.

[10] G. Myles, A. Friday, N. Davies, "Preserving privacy in environments with location-based applications," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 56-64, 2003. Article (CrossRef Link)

[11] Yi Zheng, D. Chiu, H Wang, P. Hung, "Towards a Privacy Policy Enforcement Middleware with Location Intelligence," in *Proc. of the 11th IEEE International Enterprise Distributed Object Computing Conference*, pp. 97-104, 2007.

[12] G. Pallapa, N. Roy, S.K. Das, "A scheme for quantizing privacy in context-aware ubiquitous computing," in *Proc. of IET 4th International Conference on Intelligent Environments*, pp. 1-8, 2008.

[13] G. Yee, "Using privacy policies to protect privacy in UBICOMP," in *Proc. of 19th International Conference on Advanced Information Networking and Applications*, vol. 2, pp. 633-638, 2005.

[14] Y. Kang, H. Lee, K. Chun, J. Song, "Classification of Privacy Enhancing Technologies on Life-cycle of Information," in *Proc. of The International Conference on Emerging Security Information, Systems, and Technologies*, pp. 66-70, 2007.

[15] B. Lee, H. Kim, "Privacy Management for Medical Service Application Using Mobile Phone Collaborated with RFID Reader," in *Proc. of Third International IEEE Conference on Signal-Image Technologies and Internet-Based System*, pp. 1053-1057, 2007.

[16] L.A.F. Martimiano, M.R.P. Goncalves, E.dos Santos Moreira, "An ontology for privacy policy management in ubiquitous environments," in *Proc. of IEEE Network Operations and Management Symposium*, pp. 947-950, 2008. Article (CrossRef Link)

[17] M. Maaser, S. Ortmann, P. Langendörfer, "NEPP: Negotiation Enhancements for Privacy Policies," in *Proc. of W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement*, 2006.

[18] T. Buchanan, C. Paine, A.N. Joinson, U. Reips, "Development of measures of online privacy concern and protection for use on the internet," *Journal of the American Society for Information Science and Technology*, vol. 58, no. 2, pp. 157-65, 2007. Article (CrossRef Link)

[19] C. Patrikakis, P. Karamolegkos, A. Voulodimos, "Security and Privacy in Pervasive Computing," *IEEE Pervasive Computing*, vol. 6, no. 4, pp. 73-75, 2007. Article (CrossRef Link)

[20] C. Ozturk, Y. Zhang, W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in *Proc. of 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 88-93, 2004. Article (CrossRef Link)

[21] T. Ma, Y.-D. Kim, Q. Ma, M. Tang, W. Zhou, "Context-aware implementation based on cbr for smart home," in *Proc. of Wireless And Mobile Computing, Networking And Communications*, vol. 4, pp. 112-115, 2005. Article (CrossRef Link)

[22] B.A. Price, K. Adam, B. Nuseibeh, "Keeping ubiquitous computing to yourself: a practical model for user control of privacy," *International Journal of Human-Computer Studies*, vol. 63, no. 1-2, pp. 228-253, 2005. Article (CrossRef Link)

[23] J.M. Corby, "The case for privacy," *Information Systems Security*, vol. 11, no. 2, pp. 9-14, 2002. Article (CrossRef Link)

[24] Yi Lu, W. Wang, B.K. Bhargava, D. Xu, "Trust-based privacy preservation for peer-to-peer data sharing," *IEEE Transactions on Systems, Man, and Cybernetics, Part A* , vol. 36, no. 3, pp. 498-502, 2006. Article (CrossRef Link)

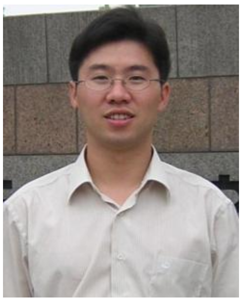
[25] G. Yee, "Measuring Privacy Protection in Web Services," in *Proc. of IEEE International Conference on Web Services (ICWS'06)*, pp. 647-654, 2006. Article (CrossRef Link)

[26] G. Pallapa, M. Kumar, S.K. Das, "Privacy Infusion in Ubiquitous Computing," in *Proc. of First International Workshop on Mobile and Ubiquitous Context Aware Systems and Applications (MUBICA 2007)*, pp. 1-8, 2007. Article (CrossRef Link)

[27] G. Pallapa, N. Roy, S.K. Das, "Precision: Privacy Enhanced Context-Aware Information Fusion in Ubiquitous Healthcare," in *Proc. of the 1st international Workshop on Software Engineering For Pervasive Computing Applications, Systems, and Environments*, pp. 10-16, 2007.

[28] S. Lederer, J. Mankoff, A. Dey, C. Beckmann, "Managing Personal Information Disclosure in

Ubiquitous Computing environments," *Technical Report IRB-TR-03-015,* Intel Research Berkeley, 2003.



Tinghuai Ma is currently working as Professor in Nanjing University of information Science & Technology, P.R. China. In 2009, he worked as visiting professor in Kyung Hee University, Korea. In 2005, he was appointed as Associate Professor at the Nanjing University of Information & Science Technology, China. He received his B.Sc. and M.Sc. in 1997 and 2000 at Huazhong University of Science & Technology, Wuhan, China. He obtained Ph.D. from Chinese Academy of Sciences, China in 2003 in Computer Software & Theory. His current research interests are Software Engineering, Data Mining, Ubiquitous Computing, Cloud Computing, and Privacy. He is a member of the IEEE-CS.

Wei Tian is currently working as Assistant Professor in Nanjing University of information Science & Technology, P.R. China. He recived his M.S. degree from Nanjing University of information Science & Technology in 2007. Now, he is a doctor candiate. His research interests are Data Mining, Data Grid Computing.

Donghai Guan received his B.S. from Harbin Engineering University, Harbin, China. He got his M.S. degree in Computer Science from Kumoh National Institute of Technology (KIT), Gumi, South Korea in 2004. He got his Ph.D. degree in Computer Science from Kyung Hee University, South Korea in 2009. From 2009, he was a Post Doctoral Fellow at Computer Science Department, Kyung Hee University. His research interests are Machine Learning, Data Mining, Activity Recognition, and Trust management.

Sungyoung Lee received his B.S. from Korea University, Seoul, South Korea. He got his M.S. and Ph.D. degrees in Computer Science from Illinois Institute of Technology (IIT), Chicago, Illinois, USA in 1987 and 1991 respectively. He has been a professor in the Department of Computer Engineering, Kyung Hee University, South Korea since 1993. He is a founding director of the Ubiquitous Computing Laboratory, and has been affiliated with a director of Neo Medical ubiquitous- Life Care Information Technology Research Center, Kyung Hee University since 2006. Before joining Kyung Hee University, he was an assistant professor in the Department of Computer Science, Governors State University, Illinois, USA from 1992 to 1993. His current research focuses on Ubiquitous Computing and applications, Context-aware Middleware, Sensor Operating Systems, Real-Time Systems, and Embedded Systems. He is a member of the ACM and IEEE.