

# UPEM: User-centered Privacy Evaluation Model in Pervasive Computing Systems

Ali Dehghantanha<sup>1</sup>, Ramlan Mahmud<sup>2</sup>, Nur Izura Udzir<sup>3</sup>, Zuriati Ahmad Zukarnain<sup>4</sup>

1 Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Dehqan@gmail.com

2 Cyber Security Lab, MIMOS, Technology Park Malaysia, Ramlan.mahmod@mimos.my

3 Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, izura@fsktm.upm.edu.my

4 Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, zuriati@fsktm.upm.edu.my

## ABSTRACT

The fact that pervasive systems are typically embedded and invisible, making it difficult for users to know when these devices are collecting data. Consequently privacy appears as a major issue for pervasive computing applications and several privacy models proposed for pervasive environments. The rapid growth of privacy models in pervasive environments gives rise to the need for some standard benchmarks and evaluation models to evaluate and compare these privacy models. In this paper we review privacy evaluation models in pervasive environments and present their evaluation results. Then we propose an evaluation model that evaluates privacy models based on user control over private information, expressiveness of privacy policies, and unobtrusiveness of privacy mechanisms and represents the model privacy level in a matrix. Finally we evaluate several privacy models using the proposed privacy evaluation model.

Keywords: Privacy, Pervasive Computing, Ubiquitous Computing, Privacy Evaluation

## 1. INTRODUCTION

PROVIDING users with enough privacy level is a basic requirement in pervasive systems which provide services seamlessly everywhere, at any time for all the users. To cope with this problem researchers propose different privacy models, each of which is capable of providing some privacy features. The rapid growth of privacy models in pervasive computing environments instigates the need for benchmarks and evaluation models for evaluating and comparing these privacy models. Because of special characteristics of pervasive environments traditional privacy evaluation models were not useful in this environment.

In this paper we review most recent privacy evaluation models in pervasive environments and propose a new user-centered privacy evaluation model. We evaluate previous privacy models using the proposed model and representing these models, privacy level using a privacy matrix.

The rest of the paper is organized as follows. In section 2 we go through recent privacy evaluation models and present their evaluation on previous models. In section 3 we describe the proposed evaluation model, we continue with evaluating previous privacy models using the proposed evaluation model. Finally the paper is concluded in section 5.

## 2. RELATED WORKS

Several privacy evaluation models have been suggested for pervasive computing systems. In this paper we review the last two privacy evaluation methods. These methods are the most comprehensive evaluations which are adaptable with recent changes in pervasive systems specifications.

### 2.1. A Practical Privacy Evaluation Method for User Control of Privacy

This research [1] introduced a layered model for the factors that affect user privacy, and based on these factors they proposed some evaluation characteristics for privacy in pervasive environment. The model consists of the following four layers:

1. Regulatory regimes layer: This layer consists of laws that affect and shape user privacy. This layer is further divided into four levels from the strictest regimes to the regimes that do not define any specification for privacy.
2. Ubicomp services layer: This layer provides query and interruption services for the third layer (data layer).
3. Data layer: This layer is divided into three sections namely static data, dynamic data and derived data. The static data are constant data that will not be changed. The dynamic data layer is divided into historical and real-time data. Historical data are those that are changing but get logged into the system so the query engine of ubicomp devices can query those data. Real time data are time dependent data used for managing interruptions. The derived data can be extracted

from static and dynamic data by analyzing and composing them.

4. User layer: This layer is the user himself.

This evaluation divides the methods of protecting privacy based on different regulatory regimes into two types:

1. Policy Matching: Comparing user privacy with that provided by ubicomp services and report mismatches.

2. Noise: Try to hide or disguise user's location or identity.

The Noise is divided into five types:

- a. Anonimizing: Hiding user identity.
- b. Hashing: Disguising user identity.
- c. Cloaking: Making user invisible.
- d. Blurring: Decreasing the accuracy of the location and time.
- e. Lying: Intentionally giving false information.

The designers classified the methods of preserving privacy based on ubicomp services into three types:

1. Prevention: Not releasing private user information if they might be misused.

2. Avoidance: Permits the release of user private information but after some steps to prevent misuse.

3. Detection: Sensing the misuse occurrence.

As the Table 1 shows this method categorized and ranked previous privacy models based on the methods of protecting privacy, types of information privacy protection, and their ability to support real time or historical data or both.

The method designers did not make any judgment on which method of protecting privacy is better than the others. Their work was valuable because of their comprehensive comparison on 10 privacy models but it was more a categorization and ranking instead of an evaluation model.

## 2.2. A Method for Measuring User Anonymity Privacy

This privacy evaluation method [12] is based on five privacy principals namely Notice, Choice and Consent, Proximity and Locality, Anonymity and Pseudonymity, and Access to Resources. The method designers gave more credits to the model anonymity and put it as a separate measurement factor called "Anonymity Assurance level". They categorized Notice and Choice and Consent principals as "Transparency of the model related to user participation" and "Response and Reactions of the mechanisms to support user privacy". Designers considered "Scalability of the model" as another factor that affects user privacy and they aggregated all other factors of Ubicomp environments such as device, bandwidth, and power consumption limitations, under "Consideration of Ubicomp Characteristics and Constraints" factor. They also considered another factor called "Theoretical justification and Validation of each mechanism" that focuses on the privacy model designer's justifications of the mechanisms that their models potentially support. Designers measure all the above six characteristics with "High", "Medium", "Low", and "None" levels. Table 2 shows the results of their evaluation on seven previous privacy models.

Researchers' fidelity to privacy principals and considering them in evaluation and their attention to some other factors like scalability are strong points of this method.

The main weak point of this method is its subjective ranking with scales like "High", "Medium", "Low", and "None" which makes the evaluation results very subjective.

## 3. PROPOSED PRIVACY EVALUATION MODEL

In this section we describe our proposed privacy evaluation model called User-centered Privacy Evaluation Model (UPEM) for pervasive computing environments. The proposed privacy evaluation model enhanced previous privacy evaluation models with additional evaluation factors and describing the method for evaluating each factor and presents the results in a matrix. In this way comparing privacy models and finding the model weaknesses will be much simpler.

Privacy can be evaluated using the following three major criteria:

1. User Control over private information
2. Expressiveness of Privacy Policies
3. Unobtrusiveness of privacy mechanisms.

### 3.1 User control over private information

The model "user control over private information" measures by the level of identity, location, and time privacy types that the model supports. To inspect user private information we have to show the model's ability to provide the above privacy types in different levels for the user.

A privacy model is able to provide User Control over Identity Privacy (UCIP) if it lets users to choose to be anonymous (Private ID), or use pseudonym identities (Protected ID), or use their real identity (Transparent ID) in communication with other parties and reliably inform other parties about the current user identity privacy policy and apply it in user communications.

A privacy model is able to provide User Control over Location Privacy (UCLP) if it lets users choose the level of location information that the other parties have access to and apply the user selected level in communications. The user should be able to select whether to not providing any location information (Private Location), or confirming existence in a certain area (Protected Location), or providing the exact location (Transparent Location) information to the other parties.

A privacy model provides User Control over Time Privacy (UCTP) if it lets users to define time periods for all of their privacy policies and control other parties' access to their time policy and guarantees the use of time policy on all communicating parties. So the model might totally hide the time of an event (Private Time), or confirm the happening within a specific period (Protected Time), or exactly provide time to other parties (Transparent Time).

The user control over private information can be shown with a flag for each privacy type and level in a way that if the model supports a level of any privacy type then the flag would be set to 1, and 0 otherwise. Therefore, User Control over Private Information (UCPI) for a model X can be shown as:

$$UCPI(X) = \begin{bmatrix} UCIP\ Real\ ID\ Flag & UCLP\ Real\ Location\ Flag & UCTP\ Real\ Time\ Flag \\ UCIP\ Confirm\ ID\ Flag & UCLP\ Confirm\ Location\ Flag & UCTP\ Confirm\ Time\ Flag \\ UCIP\ No\ ID\ Flag & UCLP\ No\ Location\ Flag & UCTP\ No\ Time\ Flag \end{bmatrix}$$

### 3.2 Expressiveness of Privacy Policies

“Expressiveness of Security/Privacy Policies” is measured by evaluating the following three characteristics of privacy models:

1. Support for Mandatory and Discretionary Rules (MDR): Pervasive environment consists of different user devices and spaces. The privacy models should be able to support mandatory rules defined by administrators as well as discretionary rules of user preferences. The model’s privacy policies should be able to reflect the model’s mandatory and discretionary identity, location, and time privacy in three levels namely Transparent, Protected, and Private.
2. Context Sensitivity (CS): Privacy rules of pervasive systems might vary based on the current context so the model should be able to support rich context information. The model privacy policies should be able to reflect context identity, location, and time privacy in three levels namely Transparent, Protected, and Private.
3. Uncertainty Handling and Conflict Resolution (UHCR): Often in pervasive environments we are in uncertain situations because of imprecise context information and imprecise nature of pervasive networks or because users with conflicted privacy policies desire to use a service or communicate with each other. So the policies should be able to detect and overcome these uncertain situations. Conflict resolution is the system’s ability to resolve these situations. The privacy policies should be able to reflect identity, location, and time uncertainty or conflict situations in three levels, i.e. Transparent, Protected, and Private. The privacy model should have mechanisms to manage conflicts in each level.

To present the model X Expressiveness of Privacy Policies (EPP) we assigned a flag which can be 0 or 1 for each privacy level of each characteristics of EPP. So EPP(X) can be reflected with the following matrices:

$$MDR(X) = \begin{bmatrix} MDR\ Real\ ID\ Flag & MDR\ Real\ Location\ Flag & MDR\ Real\ Time\ Flag \\ MDR\ Confirm\ ID\ Flag & MDR\ Confirm\ Location\ Flag & MDR\ Confirm\ Time\ Flag \\ MDR\ No\ ID\ Flag & MDR\ No\ Location\ Flag & MDR\ No\ Time\ Flag \end{bmatrix}$$

$$CS(X) = \begin{bmatrix} CS\ Real\ ID\ Flag & CS\ Real\ Location\ Flag & CS\ Real\ Time\ Flag \\ CS\ Confirm\ ID\ Flag & CS\ Confirm\ Location\ Flag & CS\ Confirm\ Time\ Flag \\ CS\ No\ ID\ Flag & CS\ No\ Location\ Flag & CS\ No\ Time\ Flag \end{bmatrix}$$

$$UHCR(X) = \begin{bmatrix} UHCR\ Real\ ID\ Flag & UHCR\ Real\ Location\ Flag & UHCR\ Real\ Time\ Flag \\ UHCR\ Confirm\ ID\ Flag & UHCR\ Confirm\ Location\ Flag & UHCR\ Confirm\ Time\ Flag \\ UHCR\ No\ ID\ Flag & UHCR\ No\ Location\ Flag & UHCR\ No\ Time\ Flag \end{bmatrix}$$

### 3.3 Unobtrusiveness of Privacy Mechanisms

The unobtrusiveness of privacy policies is the percent of time the user wastes on dealing with privacy subsystem, that is the percentage of time that user deals with privacy alarms and messages and makes decision accordingly. As a result, Unobtrusiveness of Privacy Mechanism (UPM) for the model X can be calculated as:

$$UPM(X) = \frac{\text{Total Time User Wastes on Dealing with Privacy Subsystem}}{\text{Total Working Time}} * 100$$

Better privacy models have lower UPM values.

### 3.4 Representation of Privacy Models using UPEM

Any privacy model can be shown using one matrix with four blocks as follows which are multiplied by the inverse of the UPM value as shown below:

$$UPEM(X) = [UCPI(X) \ MDR(X) \ CS(X) \ UHCR(X)] * (1/UPM(X))$$

Better privacy models have higher values in each matrix position.

In the following part we evaluate previous privacy models using UPEM evaluation.

### 4. Evaluating previous models using UPEM

#### 4.1. Loc Serve Model

The Loc Serve [15] model preserves location privacy with the use of a centralized location server that hides the clients’ location from the service providers. This model sits between the location-based and location-tracking applications to provide the required level of location privacy for location-based applications. Hence, from the “User Control over Private Information” view this model supports location privacy. The Loc Serve model did not provide any context sensitivity mechanism and it just relies on the content of XML validation tags produced by the clients to sense the context. All system rules are mandatory rules that should be conformed to by the users. Thus, from the “expressiveness of privacy policies” view point, this model only supports mandatory and discretionary rules. Defining all of the model privacy policies as mandatory rules decreased the model’s unobtrusiveness to 8.75%. This model can be shown as follows:

$$UPEM(\text{LocServe}) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} * (1/8.75\%)$$

#### 4.2. Context Model for Privacy

Context and privacy have deep relationships so the context sensitivity and context notation plays an important role in user privacy. This model [16] supports privacy through modeling the context. The uncertain nature of the context leads to the design mechanisms for managing uncertain situations and resolving conflicts.

This model relates information ownership to the context. The researchers modeled ownership of context, ownership of fact types, ownership of object type, and ownership of situations with SQL queries so that they could extract user’s privacy requirements through SQL queries of their system and

build a context related privacy preferences based on the above variables for the user.

The model defines privacy preferences with the following variables:

1. Owner preferences.
2. The requester preferences.
3. The purpose of gathering information.
4. Fact type or situation that information has been gathered in.
5. Relevant fact type attributes or situation variables.

From the “Expressiveness of privacy policies” view, this model supports context sensitivity, uncertainty handling, and conflict resolution, whereas from the “User control over private information” view it provides identity and location privacy. The high context sensitivity of the model leads to a considerable overhead for the system that increases the model unobtrusiveness, but to our knowledge there is not any evaluation on this model’s unobtrusiveness. This model can be shown as follows:

$$\text{UPEM (Context Model for Privacy)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} * (1/\text{Unknown})$$

#### 4.3. PSIUM and Anonymity Enhancer Models

These two models [17] ensure that the private information gathered by the service providers would not be misused and provide prevention of stealing sensitive information through traffic analysis (ID Privacy).

PSIUM sends some pseudo-requests accompanying real requests to the service provider to reduce the probability of guessing the real request. This model is not profitable because the user should previously possess a list of other meaningful pseudo-requests to be sent with the main one, and this results in large costs for the users. Moreover, processing these pseudo-requests incurs overhead for both the user and the service provider.

Anonymity Enhancer model followed Mix Zones model [4] in order to overcome two drawbacks: first, if a mix zone has a diameter larger than the distance a user can cover during one location update period, it might not mix users adequately; and the second is if there is no other user in the mix zone of a user, the user’s anonymous ID in that environment will be revealed to the attackers. To overcome these weaknesses the “Anonymity Enhancer” adds pseudo-users to the Mix Zones that the number of their users are less than a specific threshold so it can anonymize both the user ID and the network traffic. These techniques provide ID privacy but the added pseudo-data needs more processes and leads to a high level of unobtrusiveness.

Therefore, PSIUM and Anonymity Enhancer models do not support “Expressiveness of privacy policies”, instead they provide content, identity, and location privacy of “User control over private information” and their unobtrusiveness is 54.20%. This model can be shown as follows:

$$\text{UPEM (PSIUM and Anonymity Enhancer)} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} * (1/54.20\%)$$

#### 4.4. Tachyon Model

Nowadays RFID tags are the most well known devices in pervasive environments. Tachyon model [18] is a model to preserve location privacy for RFID tag users.

This model consists of three elements: Representation, Node, and Privacy Policy. Each RFID tag maps to a software module that is the representation of that tag. Nodes are computers, capable of detecting RFID tags with an RFID reader. Privacy policies are defined by four elements: Who, When, Where, and Delay. Who represents the person requiring location information privacy, When represents the day of the week and the time that the user wishes to expose his location information, Where represents the place that the user wants to expose location information, and Delay represents the delay time of exposing the user location information. The privacy preferences are described with XML tags. This model preserves user location privacy on each node based on the representation of each RFID tag and privacy policy of each user.

This model limited its privacy policies to only location privacy that confines to the expressiveness of privacy policies. It supports mandatory and discretionary rules without any uncertainty handling or conflict resolution mechanism. The model supports mandatory and discretionary rules of “Expressiveness of privacy policies”, Location privacy of “User control over private information”, and its unobtrusiveness is 8.45%. This model can be shown as follows:

$$\text{UPEM (Tachyon)} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} * (1/8.45\%)$$

#### 4.5. Identity-based Ring Signcryption Schemes (IDRSC)

The Identity-based Ring Signcryption Schemes [19] provides identity privacy through sign-crypt algorithms. In this way the content is signed and encrypted by a group not just one person so the real information owner that is the main signer of the information will not be revealed. The anonymity level of the system is based on the number of signers in the group and this model always guarantees that the content will be signed by enough amounts of pseudo-IDs that provide the required level of identity privacy for the users.

The public key of each participant can be obtained from his public identity such as email address or IP address combined with a username like social security number etc. This model requires a trusted authority called Private Key Generator (PKG) to generate the user’s private key after a successful user identification. IDRSC is a simplified group signature without a manager, group setup procedure, and no revocation mechanism. It provides signer ambiguity in a way that correct sign-encrypted information can convince a user that one of the signers generated that information without revealing the original signer that generates the information. The sign-encrypt mechanism is fully automated. The model designers did not propose any privacy policy format.

It can be concluded that this model does not support any factor of “Expressiveness of privacy policies”, but it supports

content and identity privacy of “User control over private information”, with 9% of “Unobtrusiveness of privacy policies”, and it is not scalable. This model can be shown as follows:

$$\text{UPEM (IDRSC)} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} * (1/9\%)$$

#### 4.6. Loom Model

The Loom model [20] preserves the content, time, location, and ID privacy of the user by keeping them in the worst and randomly chosen nodes in a tree so that their access cost will be so high for attackers with no knowledge of their exact location in the tree. The above technique can be used only for keeping data and incur considerable overhead for the system that increases the system’s unobtrusiveness. The model designers did not consider any privacy policy for the model.

Therefore, this model did not support any characteristics of the “Expressiveness of privacy policies” while it supports the “User control over private information” with high unobtrusiveness (25.50%). This model can be shown as follows:

$$\text{UPEM (Loom)} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} * (1/25.50\%)$$

#### 4.7 UPM Model

This model [21] provides location, identity, and time privacy in three levels (real, confirm, no) for five parties (user, service provider, owner, light houses, portals) communicating within three layers (user layer, service provider layer, owner layer).

This model provides privacy within five phases (authentication, context joining, service registration, service using, saving data and finish phase). The researchers claim that their model is capable of providing user identity, location, and time privacy within all phases and layers of the model although the mechanisms for providing these privacy levels are not clear. Based on their results the model’s unobtrusiveness is 7.49%. This model can be shown as follows:

$$\text{UPEM (UPM)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} * (1/7.49\%)$$

### 5. CONCLUSION AND FUTURE WORKS

In this paper we reviewed some privacy evaluation methods in pervasive computing environments and proposed a User-centered Privacy Evaluation Model (UPEM). UPEM evaluates privacy models in pervasive computing environments based on User Control over Private Information (UCPI), Expressiveness of Privacy Policies (EPP) with four factors namely support for Mandatory and Discretionary Rules (MDR), Context Sensitivity (CS), Uncertainty Handling and Conflict Resolution (UHCR), and Unobtrusiveness of Privacy Mechanisms (UPM). Finally we evaluated several privacy models using UPEM.

Our future research direction would be to enhance UPEM and include factors like scalability, and resistance against privacy attacks in privacy models evaluation.

### REFERENCES

- [1] Blaine, A. P., Adam, K., & Nuseibeh, B. (2004). “Keeping ubiquitous computing to yourself: A practical model for user control of privacy”. In *International Journal of Human-Computer Studies*, 63(1-2):228-253.
- [2] Duckham, M., & Kulik, L. (2005). “A formal model of obfuscation and negotiation for location privacy”. In *Pervasive 2005*.
- [3] Gruteser, M., & Grunwald, D. (2003). “Anonymous usage of Location-Based Services through Spatial and Temporal Cloaking”. In *Proc. First International Conference on Mobile Systems, Applications, and Services*, May 2003.
- [4] Beresford, A. R., & Stajano, F. (2004). Mix zones: “User privacy in location-aware services”. In *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops 2004*, pp. 127-131.
- [5] Hong, J. I., & Landay, J. A. (2004). “An Architecture for Privacy-Sensitive Ubiquitous Computing”. In *Proceedings of the 2nd International Conference on Mobile systems, Applications, and Services*, Boston, MA, USA, pp. 177 - 189.
- [6] Langheinrich, M. (2002). “A Privacy Awareness System for Ubiquitous Computing Environments”, In *4th International Conference on Ubiquitous Computing (UbiComp 2002)*, pp. 237-245.
- [7] Gunter, C. A., May, M. J., & Stubblebine, S. G. (2004). “A Formal Privacy System and its Application to Location Based Services”. *Privacy Enhancing Technologies*.
- [8] Jiang, X., & Landay, J. A. (2002). “Modeling privacy control in context-aware systems”. In *IEEE Pervasive Computing*, 1(3):59-63.
- [9] Lederer, S., Dey, A. K., & Mankoff, J. (2002). “A Conceptual Model and a Metaphor of Everyday Privacy in Ubiquitous Computing Environments”. Technical Report UCB/CSD-2-1188): Computer Science Division, University of California, Berkeley.
- [10] AT&T. (2004). “Find People Nearby”. Retrieved 31 January, 2005
- [11] Nguyen, D. H., & Mynatt, E. D. (2002). “Privacy Mirrors: Understanding and Shaping Socio-technical Ubiquitous Computing Systems” (GIT-GVU-02-16): Georgia Institute of Technology.
- [12] Dritsas, S., Gritzalis, D., & Lambrinoukakis, C. (2005). “Protecting privacy and anonymity in pervasive computing: Trends and perspectives”. *Telematics and Informatics*, 23(3):196-210.
- [13] Jendricke, U., Kreutzer, M., Zugenmaier, A. (2002). “Pervasive privacy with identity management”. In *Proceedings of the Workshop on Security in Ubiquitous Computing (UbiComp 2002)*, Sweden.
- [14] Muhtadi, J. Al., Campbell, R., Kapadia, A., Mickunas, M., Yi, S. (2002). “Routing through the mist: privacy preserving communication in ubiquitous computing environments”. In *Proceedings of the International Conference on Distributed Computing Systems (ICDCS 2002)*, Austria.
- [15] Myles, G., Friday, A., & Davies, N. (2003). “Preserving privacy in environments with location-based applications”. In *Pervasive Computing, IEEE*, 2(1):56-64.
- [16] Henriksen, K., Wishart, R., McFadden, T., & Indulska, J. (2005). “Extending context models for privacy in pervasive computing environments”. In *Third IEEE International Conference on Pervasive Computing and Communications Workshops 2005 (PerCom2005)*, pp. 20-24.
- [17] Cheng, H. S., Zhang, D., & Tan, J. G. (2005). “Protection of privacy in pervasive computing environments”. In *International Conference on Information Technology: Coding and Computing 2005 (ITCC 2005)*, 242-247.
- [18] Iwai, M., & Tokuda, H. (2005). “RFID-based location information management system with privacy awareness”. In *Proc. 2005 Symposium on Applications and the Internet Workshops 2005. (Saint 2005)*, pp. 468-471.
- [19] Xinyi, H., Susilo, W., Yi, M., & Futai, Z. (2005). “Identity-based ring signcryption schemes: Cryptographic primitives for preserving privacy and authenticity in the ubiquitous world”. In *19th International Conference on Advanced Information Networking and Applications 2005 (AINA 2005)*, pp. 649-654.

- [20] Imada, M., Ohta, M., & Yamaguchi, M. (2006). "LooM: An anonymity quantification method in pervasive computing environments". In Proc. 20th International Conference on Advanced Information Networking and Applications 2006 (AINA 2006), pp. 92-96.
- [21] Dehghantanha, A., Ramlan, M. (2009). "User-centered Privacy Model in Pervasive Computing Systems". In Proc. 2009 International Conference on Future Computing (ICFCC 2009), Kuala Lumpur, Malaysia.

Table 1: Privacy evaluation result of a practical evaluation method for user control of privacy [1]

Author(s)/ System Name	Description	Type of privacy protection	Real-time	Historical	Method of Protecting Privacy
Duckhan & kulik, [2]	Location blurring to nearby point	Preventive	*		Noise (Blurring)
Gruteser & Grunwald,[3]	K-anonymity	Preventive		*	Noise (Blurring/ Anonymity)
Mix Zones[4]	Provides unlinkability between pseudonyms	Preventive		*	Noise (Hashing)
Confab[5]	Privacy proxy handles digitally signed privacy metadata	Avoidance, Preventive	*	*	Matching Policies, Noise (Cloaking, Lying)
Privacy Awareness System (paws)- [6]	Use of Privacy proxy, Privacy-aware database	Avoidance, Preventive	*	*	Matching policies
AdLoc[7]	Combining formal access control with PDRM	Avoidance, Preventive	*	*	Matching policies/ access control
Information spaces-privacy tagging [8]	Model: Approximate Information Flows, the principle of Minimum Asymmetry	Prevention, Avoidance & Detection	*	*	
Faces [9]	UI Metaphor: Situational faces metaphor- conceptualizing end-user privacy preferences	Preventive	*	*	
Find People Nearby [10]	Friend finding application	Preventive	*		Noise (cloaking)
Privacy Mirror[11]	UI Metaphor: Privacy Interface (for feedback and detection)	Detection		*	

Table 2: Privacy evaluation result of “A Method for Measuring User Anonymity and Privacy” [12]

Approach	Satisfaction of Anonymity criteria	Comments	Level of Anonymity
Privacy awareness system (pawS)[6]	Low Medium Medium High None	Flexible design, adoption and co-operation with preferred anonimizing solutions; the level of anonymity is proportional to the adopted anonimizing solutions.	Flexible
Identity management [13]	High Medium Low Medium Low None	Level of anonymity offered is highly situational depended, high level of anonymity for specific environments.	Medium
Mist protocol[14]	High High Medium High High None	Offer location privacy, connections anonymity and messages confidentiality offered; drawbacks for some specific scenarios and in uncontrolled environment.	High
Mix-zones[4]	High High High High None None	Combination of frequent alterations of pseudonyms and mix-zones; its high anonymity level depends on the use of specific parameters of the mix-zones.	High
Privacy mirrors[11]	Low Low Low Low Medium None	Indirect assurance of anonymity; depends on users’ knowledge about each system and on their actions; difficult for novice users.	Minimum
Faces[9]	Medium Medium High Medium Low None	Abstract model; no implementation proposed; anonymity level depends on each proposed implementation.	Flexible
Information spaces-privacy tagging[8]	High High High High Medium None	High level of anonymity in trusted environments; based mainly on the representational accuracy presented by an object.	High

Legend: 1: advantages and limitations of anonymity assurance level as indicated by the researchers of proposing each mechanism. 2: Theoretical and specific results concerning the validation of each mechanism in practical scenarios. 3: Consideration of ubicomp characteristics and constraints. 4: Transparency of the proposal related to users’ participation. 5: Scalability of the proposed model. 6: Response and reaction of the mechanisms by supporting and offering appropriate actions to end-users, when the level of anonymity offered is below a specific threshold.