Journal of Ubiquitous Systems and Pervasive Networks
Volume 10, No. 1 (2018) pp. 11-19

Mechanism for Privacy Management Based on Data History (UbiPri-His)

Valderi R. Q. Leithardt [a, b, d] *, Luiz Henrique Andrade Correia[c] , Guilherme A. Borges[b] , Anubis G.M. Rossetto[b] , Carlos O. Rolim[b] , Claudio F. R. Geyer [b] and Jorge M. Sá Silva[d]

[a]*Laboratory of Embedded and Distributed Systems, University of Vale do Itajaí (UNIVALI), Itajaí, Brazil, 88302-202*
[b] *Institute of Informatics, Federal University of Rio Grande do Sul (UFRGS), Porto Alegre, Brazil, 91.501-970*
[c] *Federal University of Lavras, Lavras 37200-000, Brazil*
[d]*Department of Computer Engineering, University of Coimbra, Coimbra, Portugal, 3000-370*

Abstract

Privacy control and management in ubiquitous environments is not a trivial task. Especially in heterogeneous environments with different criteria and parameters related to communication, devices, users, and features of the environment itself. This work presents a study related to the algorithms that best fit the criteria, parameter, and information for the treatment of data privacy based on the user's history in the ubiquitous environment. For this, a prototype adapted to the UbiPri middleware was developed with the necessary characteristics for the historical control called UbiPri-His. They were tested, identified and identified for the mechanism for the management of data privacy related to the user's usage history, according to the environment and its location. An implementation carried out in a taxonomy, in the UbiPri middleware, and as a solution for comparison and definition of the algorithm with the best performance for the historical data file.

Keywords: *Ubiquitous computing, Privacy Management, History Control*

1. Introduction

In the last ten years, advances in mobile communication technologies have led to a change in the computing paradigm. The traditional model is static and relatively predictable with workstations and has created a highly dynamic environment with constant changes caused by user mobility. This feature is enhanced by the use of multifunctional mobile devices such as cell phones and smartphones [1], as well as educational environments such as interactions Teleduc, Moodle, etc. This change can be seen as another stage towards the concept of Ubiquitous Computing (Ubiquitous / Pervasive Computing) introduced by Mark Weiser [2], - these terms are now considered to be synonymous.

We are now living in an interconnected society, with e-mails, cell phones, Palms, chats, information search engines, news sites, online communities, SMS, IM, VoIP and other tools that until recently were not part of our daily routine either at work or leisure. According to Abech et al. [3], the popularity of mobile devices to access the Internet makes it feasible to obtain educational content regardless of time or place. In this new scenario of technological changes, there are new challenges and new forms of relationships that affect human behavior and hence all social factors involving education. Among these challenges is the question of privacy control which is of great importance since data and a shared location is unavailable without prior knowledge and authorization. This is a considerable problem given the increasing ease of access to computing resources. This kind of information can be best managed by the ubiquitous environment.

Thus, it is also necessary to have a control of privacy, since the user may not need or want to locate or share his/her data at all times. The shared information can be best managed by the pervasive or ubiquitous environment since this is a means, for example, of reducing unnecessary data processing and increasing the level of security and management of services. We are now living in an interconnected society, with e-mails, cell phones, Palms, chats, information search engines, news sites, online communities, SMS, IM, VoIP and other tools that until recently were not part of our daily work routine and leisure activities. According to [3], the popularity of mobile devices to access the internet makes it feasible to obtain educational content regardless of time or place. In this new scenario of technological changes, there are new challenges and new forms of relationships that affect human behavior and hence all social factors involving education.

Thus, a model of ubiquitous privacy control is needed that meets as many requirements as possible related to the physical and virtual environment. In the literature, several studies can be found addressing the privacy control research issue aiming

* Corresponding author. Tel.: +5547999699697
Fax: +554733417911; E-mail: valderi@univali.br

DOI: 10.5383/JUSPN.10.01.002

both: the user and the devices, services or communications employed. With regard to these features, this paper seeks to make a proposal of a privacy model for the ubiquitous academic environment, related to the real-world ubiquitous application of educational computing. Security issues will not be addressed in this ubiquitous computing, as there are already techniques to prevent attacks or disclosure of encryption information. Nor will this study address the question of the restrictive controls of users and devices, or its services and forms of communication.

The main concern of this work is the privacy model proposed for ubiquitous environments that provide definitions of parameters and criteria for an individual environment. Appropriate data classification algorithms were used for the control and privacy management environment and these were based on rules. The work is divided into the following sections: It starts with a review of related works in the literature. Following this, there is a description of the privacy settings in ubiquitous environments and a Table where a comparison is made between the proposed model and research work. After this, the application scenario is then described and then the proposed model. Finally, there is a summary of the conclusions and suggestions for future work.

2. Related Works

In ubiquitous environments, there are many problems and issues that need to be discussed, in particular, the control and management of privacy. According to Warren and Brandeis [4], privacy is intrinsically linked to the perception of each individual about what it represents, such as a threat to their personal property or physical or moral integrity.

Thus, it can be inferred that the privacy setting is something very abstract and subjective, and takes account of the diverse needs of each individual. These needs are not homogenous and may depend on cultural areas such as religion, tradition, customs, education or politics, or more subjective concerns such as user privacy or everyday factors such as age, health status, job responsibilities, mood, and leisure activities.

According to Cristiano et al. [5] data that characterize a context may range from the physical world to the virtual world, and sometimes the two are merged. People often do not think of physical environments (e.g. an office, shop floor, stadium, and classroom) and virtual environments (e.g. a desktop computer, or the features of a mobile phone) as separate areas [6]. Thus, the problem becomes even greater owing to the interaction between devices, users, applications, and communications between these environments. The work of [7] involves the transfer of the control of music files based on the location of WIFI points. This author offers a different interpretation to what is given in this study He seeks to define the types and sizes of information that must be transferred with regard to section and location. However, in our view, the question does not concern the environment itself but the point of access to it. Thus, it is necessary to couple several other systems supply information about the ubiquitous environment, and hence how it should proceed [8].

Henricksen et al. [9] describe the hierarchy of control based on facts and user preferences. They also describe a context model of the application that controls the facts and individual occurrences, by seeking information on various ubiquitous sources; thus, it is not the privacy control in the ubiquitous environment.

The work described by Iachello and Hong [10], conducts a survey of several privacy issues addressed in the context of human-computer interaction (HCI); the work also provides an overview of several points that should be tackled such as trends in the field and research being carried out. The main contribution of this work is that it addresses several key issues including the protection of the pervasive environment.

In Bardram, Kjaer, and Pedersen [11] an authentication-based solution is provided that is based on several examples of communication such as Radio Frequency Identification (RFID) and offers a single mechanism to manage different authentication protocols in ubiquitous environments. Despite carrying out authentication iterations with the pervasive system, there is not a change of perspective in the environment, nor any attempt to address issues related to individual privacy.

The work of Santarosa, Comfort, and Basso [12] seeks to support digital social inclusion in the technological dimension including principles of accessibility. This exposes many points of weakness in the virtual learning environments, in particular, the privacy control system in the devices used. In Tao and Peiran [13] there is a research inquiry into the protection of data for individual transactions between users and "things" (Internet of things, IOT), based on the use of cards, tags and other devices of everyday use.

It also outlines some specific situations in which IOT is used with categories and applications where concepts are defined in terms of a specific situation: for example, medical treatment is defined as private identification, but only based on the user´s location and restricted to the pervasive goal. In the work carried out by Gotardo and Zorzo [14], there is an examination of the technologies that assist in the process of teaching and learning which are being discussed in various fields of knowledge where the issue of privacy is handled by a user agent. In the work developed in [23], it contributes to research-related solutions primarily to the services provided. Based on the previously-presented research studies, a comparison is made in Table 1. The left column has abbreviations and the number of references that are cited. The tables' first line outlines the approaches required for privacy management in pervasive environments. The following definitions are used:
(i) Addresses (A): the work deals with the Question addressed; (ii) It does not address (NA): The work does not deal with the Question addressed; (iii) Not describes (ND): information not found to address the question; (iv) Developing (D): The item is still being developed; it is often pointed out in tests, validations, obtained results or future work.

Table. 1. Comparative of Privacy Management Approaches in Ubiquitous Environments

Approach	User	Device	Application	Services	Communication	Environment	Privacy
[8]	A	NA	A	D	A	D	NA
[6]	A	NA	A	A	A	NA	NA
[7]	A	A	A	NA	D	NA	NA
[23]	D	NA	A	A	A	ND	D
[9]	D	D	A	A	D	NA	NA
[10]	NA	ND	D	D	A	NA	NA
[11]	A	D	A	A	A	NA	NA
[12]	A	D	D	NA	NA	D	NA
[13]	D	A	D	A	D	NA	D
[14]	A	D	A	A	D	NA	D
Proposed Model	A	A	A	A	A	A	A

Several of the presented studies describe the particular solution that applies to a pervasive or ubiquitous environment, nevertheless, they do not state clearly how to go about the management and control of ubiquitous environments. In this way, the next section will examine the application scenario where the privacy management model in ubiquitous environments is applicable.

3. Middleware

In this section, the proposed model for privacy management in ubiquitous environments is illustrated in Figure 1. It is based on the following requirements:(1) the support of privacy management based on each criterion previously presented – i.e., User, Device, Application, Communications, Environment, and privacy; (2) there is a need to collect personal information to operate these systems regarding the ethical and legal constraints, because the privacy of people is involved; (3) the software functions of the user tracking, decision making and adaptations to support the privacy management.

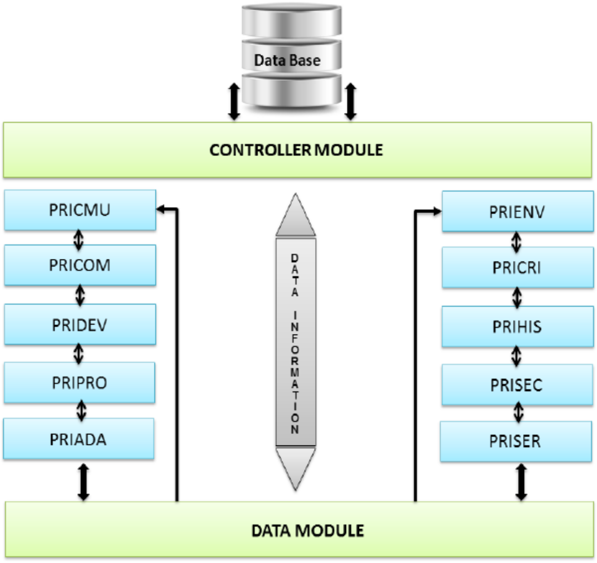


Fig. 1. Model of Privacy Manager [15].

Base on such requirements, the proposed model consists of several components to enable the control of ubiquitous environments. They can be individually described as follows:

Data Base: Rules for Information Storage and settings for users, devices, and the ubiquitous communication environment. This database acts as a single register of species containing all necessary information for the control and management of privacy mechanism in ubiquitous environments.

Controller module: the purpose of this is to receive access requests and perform the database control of the tables directly, with necessary information in accordance with the requests and access settings and by maintaining control of the ubiquitous environment. This module also performs validation requests and updates the database after the information has been returned to the calculated and refined module before being sent on to the control module.

Data Module: In this module, calculations will be made of all the variables and parameters received from the other modules. Its function is to receive and handle a wide range of data to generate single output information for each processing run.

PRICRI: this module contains the rules and definitions of criteria and environmental settings such as access, use, sharing, location and other variables that can be manipulated or replaced in accordance with a) the environment settings and b) established criteria and standards;

PRICMU: Module management and privacy control of user information, which will handle definitions of related features for individual user preferences such as temperature, light, authorized shares (such as information that someone wishes to share with other users and with his/her own environment), location data and other user preferences.

PRIDEV: management module and privacy control devices. This module will handle the data on the devices if these devices are in the environment itself and will then interact with it. Management and control refer to the software and hardware features of each individual device, such as size, weight, screen resolution, operating system, means of communication, etc.

PRICOM: management module and communications privacy control. This concerns which forms of communication will be employed within the ubiquitous environment and how they will be used. These include sign restrictions and the type of adapter used which can serve as an access controller, as in the case of the environment in the real world, where certain environments have only one type of communication.

PRIADA: management and adjustment control module. This module will handle the information related to the adaptation of software and hardware in ubiquitous environments. For example, the content and media may not have the same performance and functionality owing to issues such as size, communication, configuration, among other features.

PRISER: environmental services management module. This module is responsible for the availability of services that can be used individually in each environment such as, shared information from other environments, devices, communications, the location of users, environmental availability and its components that interact with users.

PRIHIS: this module will store and handle information on the historical user, environment, devices and other variables that may include other factors depending on the context. The operating characteristic is based on the use of information that is picked up over a given period of time and based on other sources of information such as multitrack, context, etc.

PRIPRO: this module will carry out transactions of controls related to the user profile management.

PRISEC: this module will carry out the controls and management with regard to the safety of both the user and environment. Its function is to receive the parameters and settings related to data encryption or other security-related matters and forward them to the applicant in accordance with the needs of each situation. For example, when entering a given environment, the user may find the date and time are not allowed for him in this environment.

PRIENV: this module will register the attributes related to the environment. This information enables someone to check and manage what makes up the environment, (and its capacities and capabilities) so that the resources and services can be shared with users who need them (depending on their availability).

All the modules operate independently and have their own characteristics and features that may vary according to the rules that have been previously established registered and enforced [15]. Once these rules have been set out, each module sets its parameters based on the settings of the previous module.

Thus, it is possible to have multiple environments with different rules and definitions for the same ubiquitous environments and the same user can use one or more different environments each with a defined criterion. This can change depending on the device used in the communication as well as other factors that will be calculated on the data module.

3.1. Taxonomic model of privacy

The Taxonomy presented in Figure 2 was designed to support the proposed control and privacy management, model. It also describes the necessary requirements to address privacy in ubiquitous environments. Among the research projects that address privacy, references were consulted that designed their own taxonomies for handling users, devices, applications, and communication, especially the use of protocols, treatment services, and ubiquitous environments. Thus, in this section, we list the main contributions of the papers regarding their ability to describe and define a taxonomy for control and privacy management and thus be able to set out the parameters and items needed for use in ubiquitous environment.

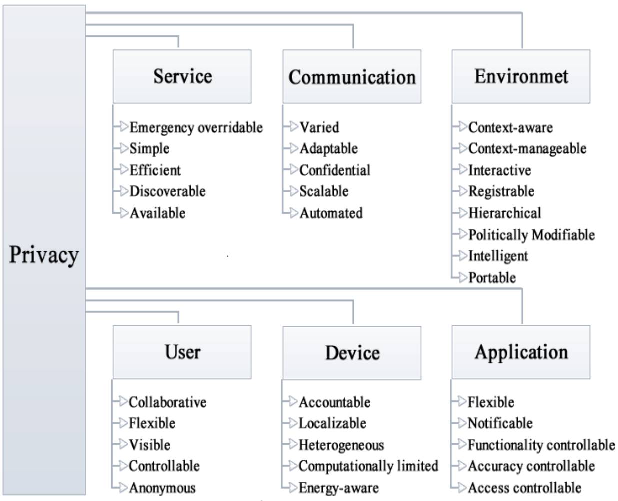


Fig. 2. Taxonomic model of privacy [26].

As shown in [26] the taxonomy needed for use in ubiquitous environments was divided into 6 groups: User, Device, Application, Services, Communication, and Environment. Each group has specific features that can be employed as needed, such as: if the User needs to be collaborative, there is an interest shown among others; it must be flexible so that an exchange of information is visible to others in the same environment; it must be controllable so that other users are able to superimpose their own preferences; and anonymous in certain situations where there is a need for privacy.

The application group is concerned with issues relating to the operation control and management of the application, unlike the group responsible for the services provided. On the basis of the taxonomic settings, the next section will outline the prototype and examine the preliminary results.

4. Prototype testing and preliminary results

The implemented prototype, illustrated in Figure 3 shows the scenario used where the privacy settings server (4), (which acts as an authority for the mobile devices (2) and environments), receives the inferred symbolic locations through physical locations (1) and the mobile devices that the users upload. Each mobile device can be used by a unique user at the time; though, they can be used by more users at different times. Thus, the server performs the model described in the previous section and identifies which adaptations must be applied to the user's device regarding the criterion of environmental privacy. Once conclude this process, the server informs the mobile device via the communication channel (3) which actions they must perform.

The server and the model are implemented using Java EE programming language, which currently supports communications WebService Rest, Google Cloud Messaging (GCM) and Serial Communication. A PostgreSQL relational database was also employed. An implementation of mobile device devices using an Android platform, the mobile clients were built for the Android platform, and their native APIs were used for access to information about the location. The prototype currently:

➔ Makes environmental changes using different locations such as GPS and NFC Tags;

➔ Identifies what types of access each user profile possesses when entering an environment;

➔ Enables or disables the smartphone functionality in accordance with the privacy required by the environment.

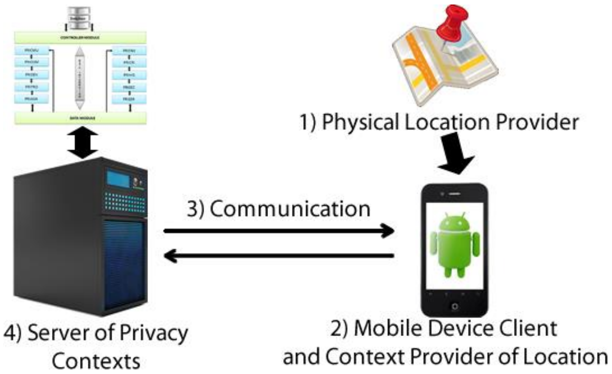

1) Physical Location Provider
3) Communication
4) Server of Privacy Contexts
2) Mobile Device Client and Context Provider of Location

Fig. 3. Implemented Architecture.

One problem was how to classify the degree of access that a user has to the environment. This problem was solved by identifying the variables that provide the level of access required by the user to the environment, which are as follows: Profile and user frequency in the environment, an environment, weekday, shift and working day. Six profiles were considered for possible user profiles in each environment, as each room has the following different interactions for each user:

- Unknown: User is unknown to the environment.
- Transient: Profile of person that only accesses when passing through the environment or is a temporary visitor.
- User: Profile of users who interact with the environment more intensely. They are often present in the environment for a considerable time or use services provided by the environment.
- Responsible: Responsible or local official, has more rights of access or permission than the customers and the like.
- Student: student profile, someone who has different rights of access from ordinary users and staff.
- Manager: This is the highest authority of the environment. He has maximum rights of access and can add, remove and change users, and can modify the profile of each environment.

The first three profiles (Unknown, Transient and User) are automatically identified and allowed to proceed through the system (evolutionary profiles), while the last three

(Responsible, Student and Manager) are assigned manually by the environmental manager. This configuration is necessary because a large number of users will probably not access all the environments known by the system. In this way, the system itself can distinguish between ordinary and new users while it is running, thus dispensing with the settings of the system manager. By contrast, ordinary users will not be able to access all the resources, especially in private settings, or automatically be allowed to proceed for security reasons. For example, the customer in a cafeteria might not be able to access the box, as such, since there are profiles that have to be assigned to the user manually.

The rules for the progression of evolutionary profiles are configurable in the system. In this study, the frequency (F) of the user (u) is used to determine when it should evolve into a profile (R) before it can advance through the environment or be resolved as a less permissive profile. In this case, for each environment, the implemented rules define, (a) the location of the lower frequency ranges (I) and upper (S) at which a change of profile should be made. If the environment has no evolutionary profiles, the equation below expresses the progression rule that is implemented.

Pu,a=Pu,a+1, if Fu,a>Sa; Pu,a-1, if Fu,a<Ia ; Pu,a, otherwise: P [1,n]

In the case of non-evolutionary profiles, the frequency is also used to increase or reduce the level of access to users. However, the user profile remains the same and only the type of access is changed. In both cases, it was assumed that the frequency can take on three distinct levels: frequent, normal and infrequent.

Three types of environment were also taken into account: restricted, private and public; it is assumed that the binary value is true for weekdays, and false, for weekends; There were two shifts, day and night; Finally, the variable working day indicates whether a day is useful or not with regard to the location based on the day of the week or holidays since there are no days which have working hours for certain environments. The combination of all the variables that are possible in the case scenario studied resulted in a rating with 383 possibilities.

In the second instance, after being identified, the variables were assigned to the combinations of the following types of access: Locked, Guest, Basic, Advanced and Administrative. These data were used for training and testing in seven different classification algorithms (Table 2), to determine the one with the highest degree of accuracy. These experiments were used to select the algorithm that could be used by the server to automatically classify the user access level in unfamiliar surroundings and that had not been configured in the system, or in other words, where all the rules of a well-defined environment can be found.

The comparative experiment between the classification algorithms was carried out by Weka tool [16] [17]. The Table with the rules (a combination of all the attributes and their types that result in access) was divided into training and testing sets, through a cross-validation technique with ten subsets (10-fold cross-validation) [18] where 90% of the data is used for training the classification algorithms, and the remaining 10% is used to check the results of these rules (unknown to the classifier). In addition, with this method, the test set is varied among all the possible data training subsets. The final degree of accuracy shown in Table 2 is obtained from the average of the tests.

Table. 2. Comparison of Classification Algorithms

Algorithm Classification	Precision	Correct Instances	Incorrect Instances
Decision Table	0.887	343	40
Bayes Network	0.814	322	61
J48	0.887	341	42
Best-First Decision Tree (BT-Tree)	0.871	336	47
Random Tree	0.861	332	51
Nearest Neighbor With Generalization (NNge)	0.848	326	57
Multilayer Perceptron	0.888	341	42

An ontology was designed to formally represent the UbiPri model, [19]. This ontology consists of classes described in Figure 3 and properties described in Table 3. According to [20], ontologies can be used to represent the context, provide inferences and share the knowledge generated by the application. Similarly, [21] X states that axioms, bodies, and vocabulary can be shared with the scientific community.

Table. 3. Ontology data UbiPri

Item	The Amount
Classes	45
Property Objects	11
Data Ownership	3

FOEval assessment and evaluation scenarios were used to validate the ontology. FOEval allows users to select a set of metrics that can assist in the evaluation of ontologies. For this study, metrics were chosen with a level of detail and computational efficiency recommended by [22].

Three calculations are made to assess wealth. First, the wealth ratio (RR) measures the range of relationships and assumes that the higher the number of non-hierarchical relationships, the richer the ontology. Another calculation performed is the wealth attribute (RA) which is the average number of attributes that are defined for each class. This may indicate the amount of information in the instance data, since the more attributes are set, the greater the amount of knowledge the ontology conveys. Finally, the rich ontology is calculated (RO) from the RR and RA values.

According to [22], RO is set to the sum of RR and RA. RR is defined as the ratio between the numbers of non-hierarchical relationships defined in the ontology, divided by the number of all the (R) attribute wealth relations. RA, in turn, is defined as the number of attributes defined for all classes divided by the number of ontology classes. To make the calculations of the ontology, data were used (as summarized in Table 3). The results obtained for the ontology were UbiPri points for RR 1.27; 0.31 points for RA; and 1.58 points for RO. These results demonstrate that UbiPri ontology is richer in relationships than in attributes. Furthermore, there is, on average, 15 classes by attribute and a relationship of 3 classes.

The overall level of detailed calculation is defined by the average number of subclasses divided by the number of ontology classes. When we make to obtain the total number of subclasses, including 45 classes. We come to near zero, 0.02 ((48/45) / 45 = 0.02)). UbiPri ontology is divided in terms of classes and subclasses and is very close to midway between the vertical and horizontal types of the taxonomy.

The calculation of the computational efficiency considers the possibility of ontology UbiPri growing 10 times, that is, the data on the number of classes, instances, and other elements can be multiplied by 10. According to [22], the computational efficiency can be defined as (number of classes of evaluated ontology [content?]/ greater number of classes of a candidate ontology) + (number of subclasses of all classes of the ontology + number of evaluated ontology relations) / number of classes evaluated ontology) + (number of evaluated ontology relations) / (greatest number of relations of a candidate ontology) + (size in kilobytes of evaluated ontology) / (size in kilobytes of candidate ontology). Applying the formula, we obtain the value 4.54. The values considered were: (45/450) + ((48 + 14) / 45) + (14/140) + (47/470). The computational efficiency proved to be easily processable in spite of the simulated growth since its value was relatively close to zero. A better understanding of the rules, definitions, and criteria used for the control and privacy management (as also represented in the described ontology) is provided in the application scenario section that follows.

5. Application Scenario

When used in an application scenario the traffic information data was taken into account and controlled in accordance with the rules and specific criteria of the environment. Thus, the evaluation scenarios can be represented by instances as shown in Figure 4 and according to the information described in Table 5. This is described as follows: "Carlos is an employee of the university and is responsible for the warehouse management of the University. One Thursday on 04/05/2015 at 02: 00h., Carlos decided to study in the Information Technology Institute, known by the community as inf, but was not sure if he could have access to the institute because of the privacy policies for UbiPri being implemented by software. In view of this, Carlos accessed the UbiPri system through the university website and found out, that according to the inferences applied to the current situation of Carlos, that to have access to this environment, it would have to have Advanced permission, the restrictions of which are described in Table 6. As Carlos had this type of access, he could study in the environment at that time. ". After obtaining the type of access to the environment, it can decide what actions should be sent to the device used by the user, starting with the default actions for each feature and also take account of the standard rules and type of environment. Each instance corresponds to and there is a feature that may be assigned to the user device and which varies according to the day of the week, shift, location, etc. that can have variations. This can be considered a level of access that results from the type of user access in the environment and the type of accessible environment.

The Table with the rules (combination of all the attributes and their types resulting in access), was divided into training and testing sets, through a cross-validation technique with ten subsets (10-fold cross-validation), where 90% of the data is used for training the classification algorithms, and the remaining 10% is used for checking the results of these rules (unknown to the classifier). In addition, with this method, the test set is varied among all possible subsets of the training data. The final degree accuracy is shown in Table 4 and is obtained from the average of the tests.

Table. 4. Classification and definition of environmental criteria

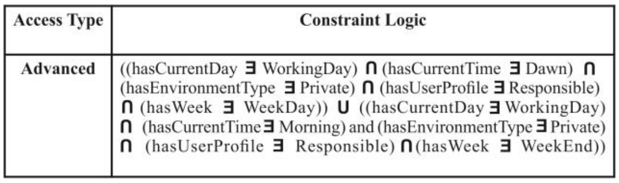
Property	Features	Domain	Range
hasUser	Funcional, Transitive inverseOf isAtEnvironment	Environment	CurrentUser
hasAccessType	Funcional, Transitive	Environment	AccessType
hasCurrentDay	Funcional, Transitive	Environment	CurrentDay
hasCurrentTime	Funcional, Transitive	Environment	CurrentTime
hasEnvironment Type	Funcional, Transitive	Environment	Environmen Type
hasLocation	Funcional, Transitive	Environment	Location
hasResources	Transitive	Environment	Resources
hasUserProfile	Funcional, Transitive	Environment	UserProfile
hasWeek	Funcional, Transitive	Environment	Week
isAtEnvironment	Funcional, Transitive inverseOf hasUser	Current User	Environment

6. Example of use and preliminary results

In the experiments, the functions were tested and validated in 5 partially registered environments; both were considered for 5 users, with the features registered in a differentiated way for each of them. For example, there were schedules, access to certain environments and functions of different devices. The tests were performed on two real devices with an Android operating system and also made use of the emulators available for the Android platform. If applicable, the actions that should be applied to the device are based on the number of parameters. This procedure begins with the user's mobile device when it detects that the user has entered or left the room.

Once the detection has been made, the user device sends a message to the server with environmental identification, in addition to the user´s ID and device. On the basis of this information, the server obtains the information on the user from the database and his device, as well as the rules set for the user within the environment in which the input and output are registered. If these rules have not been set, (which occurs when the user enters the first environment), the server will be responsible for creating the rules with predefined parameters. With all this information stored, the server updates the current location of the user and his device, and creates a log in the database, to describe the event that has just occurred. If the user is outside of the environment, there is no need to continue the procedure, as the next stages are for the definition of actions that must be applied to the device when it enters a room.

Table. 5. Restrictions on the type of access to an advanced ontology



Access Type	Constraint Logic
Advanced	((hasCurrentDay ∃ WorkingDay) ∩ (hasCurrentTime ∃ Dawn) ∩ (hasEnvironmentType ∃ Private) ∩ (hasUserProfile ∃ Responsible) ∩ (hasWeek ∃ WeekDay)) ∪ ((hasCurrentDay ∃ WorkingDay) ∩ (hasCurrentTime ∃ Morning) and (hasEnvironmentType ∃ Private) ∩ (hasUserProfile ∃ Responsible) ∩ (hasWeek ∃ WeekEnd))

6.1. Generic Privacy Taxonomy Model

The server is responsible for receiving the contextual location information and deciding what actions should be carried out by this device in the environment, depending on the type of user and type of environment. Two classes are used for both the current implementations (Communication and Ubiquitous Privacy Control) and a type of UbiPri middleware decision-making shown in Figure 5, which are described below:

→ WebServiceRestCommunication class receives a remote call using the Rest WebService technology through one of the following methods: onChangeCurrentUserLocalization (if the call is asynchronous) or onChangeCurrentUserLocalizationW ithResponse.

In both cases, the incoming parameters are login, user password, the source device to the location, the environment identifier and an optional parameter indicating whether the user is entering or leaving a room. The information of this method is then passed to the Communication class.

→ The Communication class has methods of the same name used for receiving messages. It is also responsible for sending messages originating from the Ubiquitous PrivacyControl. This setting is chosen because it is possible to use different communication technologies simultaneously for sending and receiving information.

After receiving the parameters of calls onChangeCurrentUser Localization with response and onChangeCurrentUser Localization parameters are passed on to the PrivacyControlUbiquitous class through methods onChangeCurrentUser Localization ReturnActions and onChangeCurrentUser Localization WithReturnAsynchronousActions through the same process of sharing decision-making and differentiating the way to return to action.

The decision-making process, which has been described previously, was implemented in the following stages:

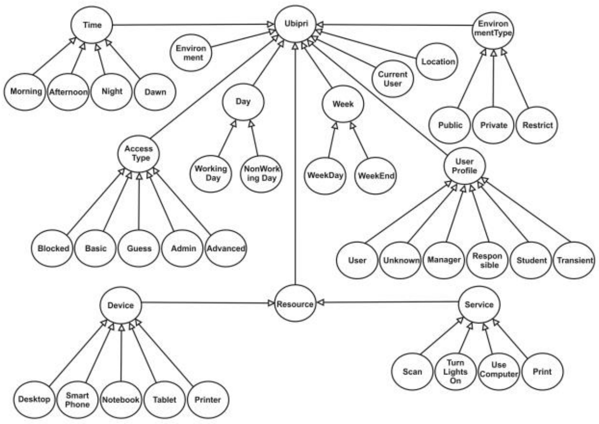


Fig. 4. Implemented Ontology data UbiPri.

a) authentication: authenticating the user, identifying the user and registering the device;

b) data search: Search the environmental information, the device and user information and one´s profile in the environment (Unknown, transient, user, student, responsible and administrator or manager);

c) generation of control: this generates a log of position change and identifies whether the current moment is a day or night shift, whether a weekday or the weekend and whether it is daytime or not.

The information handling requires a rating based on all N possibilities, considering some variables like the user profile of environmental, the type of environment, the shift, if it is holiday or if it is a business day. Some of these are described in Table 5 and define the type of access that the user has to the environment. The type of user access environmental information and the type of environment, make it possible to obtain the list of actions that can be applied to the target device. These are described as features, since the default actions may be overridden by custom if there is any room for that. Sending an action to devices using the Communication class is asynchronous, whereas returning the method is synchronous. This means that algorithms are used with mathematical functions and calculations related to artificial intelligence to run these variables and individual environmental parameters, user, devices, services, profiles, etc. The mathematical function that meets the requirements and necessary functionality is defined as follows:

$$S(r,c)=A_{r,c}$$

Where S corresponds to the service available such as the features that are not offered by the user device itself and that may be available in the environment in which it finds itself. These services are directly related to the profile that the user has defined and the criteria assigned to him. The letter R represents the resources available in the environment which can be activated by the user, such as the activation of an air conditioner, automatic driving lights in the environment, etc. The variable C matches the criteria assigned to the user and is in accordance with the definitions and rules of the location and the environment. Finally, the variable A is assigned to Table 4 of the rules and criteria for each environment. Since each environment has rules, criteria and different settings for devices, different users, it means that a Table with basic settings is required for the control and managing of privacy.

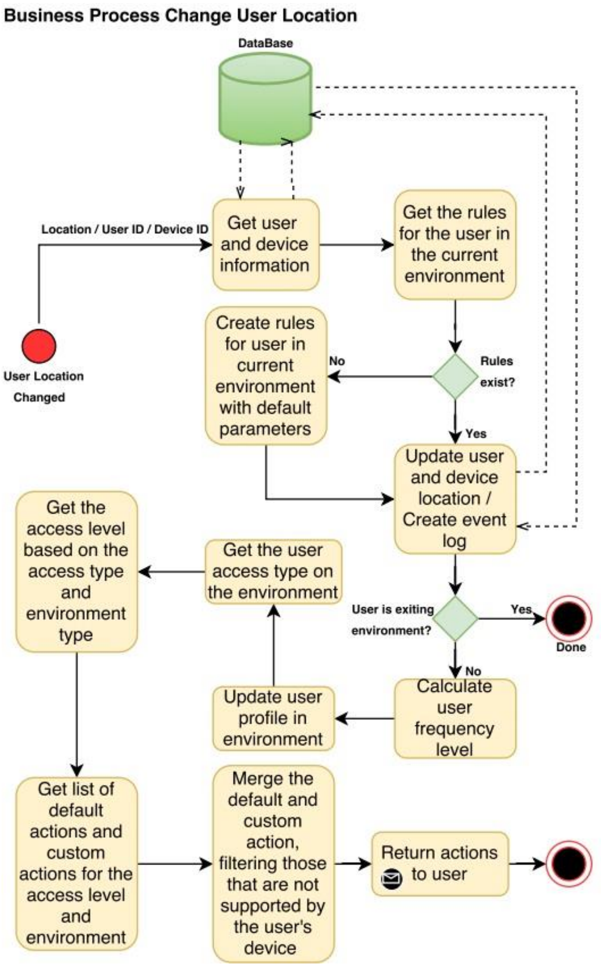

Business Process Change User Location
DataBase
Location / User ID / Device ID
Get user and device information
Get the rules for the user in the current environment
Create rules for user in current environment with default parameters
No
Rules exist?
Yes
User Location Changed
Update user and device location / Create event log
Get the access level based on the access type and environment type
Get the user access type on the environment
User is exiting environment?
Yes
Done
No
Calculate user frequency level
Update user profile in environment
Get list of default actions and custom actions for the access level and environment
Merge the default and custom action, filtering those that are not supported by the user's device
Return actions to user

Fig. 5. Business process on the user's change of location.

7. Conclusion and Suggestions for Future Works

New solutions are constantly being found involving databases, computer networks, operating systems and several other computational mechanisms which can identify users, devices, and locations without any human iteration [27]. A wide range of data and information have been drawn on to yield results that can also be used by other researchers. The scientific investigations showed that it is possible to set criterion, parameters, and variables that comply with the particular rules of each environment. Thus, it can be concluded that it is also the basis of information that is handled automatically. In this study, a comparison was made of classification algorithms for data privacy treatment and these were focused on the environment. With this, it was possible to conclude the algorithm that covers the best characteristics of the privacy criteria in ubiquitous environments. However, a good deal of further research and implementations are required in the future, due to a large amount of information that needs to be controlled and managed in ubiquitous environments. The results were generated from real data and in real-world scenarios and were based on information about students at an academic institution. This involved listening to lectures and taking part in other events in classrooms and the auditorium. We carried out a simulation to test the same settings with thousands of students, but due to several factors such as time and physical resources, it was not possible to simulate. For this reason, this fact can be listed among many others as areas for the continuation of research into data privacy in the future which should be of value in computer studies. Figure 6 shows the location, identification, and classification of the environment used in the tests. It was concluded from this that the behavior of algorithms chosen for a sample of 500 users achieved the expected results.

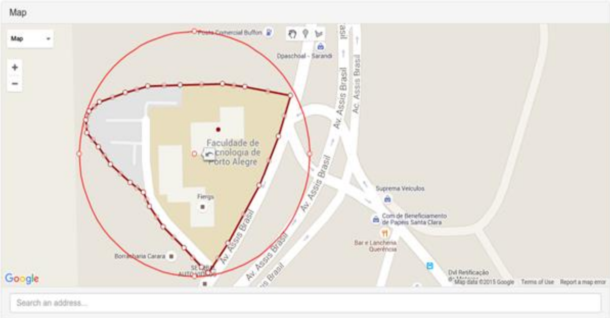


Fig. 6. User identification and environment.

In future works, we plan to simulate larger environments, with a greater number of users, devices and criterion definitions than what was used to obtain the results of this work. For this reason, two projects have been submitted to funding agencies of Brazil requesting financial assistance for further studies. This will enable us to identify and develop more robust algorithms for the handling of private data on a large scale. Other important factors also need to be considered for future work, including the following:

- Definition of data processing techniques on a large scale
- Devising computational metrics for a database
- Preparation of other environmental ratings, for example, those restricted to individuals
- Implementation of distributed algorithms for processing information
- Definition of bug tracking techniques, as well as others that will be determined in the course of the research.

Acknowledgments

This work forms part of the UbiArch project - Ubiquitous Architecture for Context Management and Application Development of the Federal University of Rio Grande do Sul. It is also part of the ongoing Post-Doctoral project: Control and History Management based on the privacy of ubiquitous environments. Developed in the Department of Computer Engineering of the University of Coimbra - Portugal. We would like to thank the National Council for Scientific and Technological Development (CNPq) for its support and also the Laboratory of Embedded and Distributed Systems (LEDS) the UNIVALI - Brazil.

References

[1] Leithardt, V. R. Q., Rolim, C., Rosseto, A., Geyer, C., Dantas, M. A. R., Silva, J. S., Nunes, D. (2012) "Percontrol: A pervasive system for educational environments". In Computing, Networking and Communications (ICNC), 2012 International Conference on, pp. 131-136. IEEE. https://doi.org/10.1109/ICCNC.2012.6167396

[2] M. Weiser, "The computer for the twenty-first century." Scientific American, vol. 265, no. 3, pp. 94–104, September 1991. Access in: https://www.lri.fr/~mbl/Stanford/CS477/papers/Weiser-SciAm.pdf - Acess in Nov 2017.

[3] Abech, M., da Costa, C. A., Barbosa, J., Rigo, S., and Cambruzzi, W. (2012) "Um Modelo de Adaptação de Objetos de Aprendizagem com foco em Dispositivos Móveis". In Anais do Simpósio Brasileiro de Informática na Educação.

[4] Warren, S. D., and Brandeis, L. D (1890) "The right to privacy". Harvard law review, 193-220. Access in: http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf - Acess in Nov 2017. https://doi.org/10.2307/1321160

[5] Cristiano Andre da Costa, Adenauer Correa Yamin, and Claudio Fernando Resin Geyer. 2008. Toward a General Software Infrastructure for Ubiquitous Computing. IEEE Pervasive Computing 7, 1 (January 2008), 64-73. DOI=10.1109/MPRV.2008.21

[6] Rodrigues, Vagner, J. d. S. (2006) "Privacy Management to Context-Aware Applications on Mobile Networks". Pontifical Catholic University of Rio de Janeiro (PUC-Rio), PhD Thesis, 136 pag. Access in: http://www.inf.ufg.br/~vagner/publications/Tese-2006-Vagner.pdf Acess in Jan 2017.

[7] Görlach, A., Heinemann, A., and Terpstra, W. W. (2005) "Survey on location privacy in pervasive computing". In Privacy, Security and Trust within the Context of Pervasive Computing, pp. 23-34. Springer US. https://doi.org/10.1007/0-387-23462-4_3

[8] Leithardt, V.R.Q.; Geyer, C.; Sá Silva, J.; Silva, R., "Use of Data Replication in WSNs Directed to Special Needs," in Communications Workshops (ICC), 2010 IEEE International Conference on, vol., no., pp.1-5, 23-27 May 2010 doi: 10.1109/ICCW.2010.5503914 https://doi.org/10.1109/ICCW.2010.5503914

[9] Henricksen, K., Wishart, R., McFadden, T., Indulska, J. (2005) "Extending context models for privacy in pervasive

computing environments”. In Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on, pp. 20-24. IEEE. https://doi.org/10.1109/PERCOMW.2005.36

[10] Iachello, G., and Hong, J. (2007) “End-user privacy in human-computer interaction”. Foundations and Trends in Human-Computer Interaction, v. 1, n. 1, pp. 1-137. https://doi.org/10.1561/1100000004

[11] Bardram, J. E., Kjær, R. E., & Pedersen, M. (2003) “Context-aware user authentication–supporting proximity-based login in pervasive computing”. In UbiComp 2003: Ubiquitous Computing, pp. 107-123. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-39653-6_8

[12] Santarosa, L. M. C., Conforto, D., & Basso, L. d. O. (2010) “Eduquito: Ergonomia Cognitiva para a Diversidade Humana”. In: Educação, Formação Tecnologia, v. 3, p. 4-13. ISSN 1646-933X.

[13] Tao, H., Peiran, W. (2010) “Preference-Based Privacy Protection Mechanism for the Internet of Things”. In Information Science and Engineering (ISISE), 2010 International Symposium on, pp. 531-534. IEEE. https://doi.org/10.1109/ISISE.2010.135

[14] Gotardo, R. A., Zorzo, S. D. (2007) “Tratamento da Privacidade dos Usuários de Sistemas Educacionais Web”. In XII Workshop de Informática na Escola, v.1, n. 1. Anais SBC.

[15] Leithardt, V.R.Q., Borges, G.A., Carrera, I.M., Rossetto, A.G.M., Rolim, C.O., Nunes, D., Silva, S.J., Geyer, C.F.R. (2013) “Mobile Architecture for identifying users in Ubiquitous Environments Focused on Percontrol”. In: UBICOMM 2013, The Seventh International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, p. 145-151.

[16] Hall, Mark, et al. "The WEKA data mining software: an update." ACM SIGKDD explorations newsletter 11.1 (2009): 10-18.

[17] Holmes, Geoffrey, Andrew Donkin, and Ian H. Witten. "Weka: A machine learning workbench." Intelligent Information Systems, 1994. Proceedings of the 1994 Second Australian and New Zealand Conference on. IEEE, 1994. https://doi.org/10.1109/ANZIIS.1994.396988

[18] Kohavi, Ron. "A study of cross-validation and bootstrap for accuracy estimation and model selection." Ijcai. Vol. 14. No. 2. 1995.

[19] Gruber, T. R. (1993). A Translation Approach to Portable Ontology Specifications. Knowledge Acquisition, 5, (2):199-220, 1993. https://doi.org/10.1006/knac.1993.1008

[20] N. Guarino. 1998. Formal Ontology in Information Systems: Proceedings of the 1st International Conference June 6-8, 1998, Trento, Italy (1st ed.). IOS Press, Amsterdam, The Netherlands, The Netherlands.

[21] Freitas, J.M.: Continuity of SRB measure and entropy for benedicks-Carleson quadratic maps. Nonlinearity 18(2), 831-854 (2005). https://doi.org/10.1088/0951-7715/18/2/019

[22] Bouiadjra A B. (2011) FOEval: Full Ontology Evaluation In proceeding of: 7th International Conference on Natural Language Processing and Knowledge Engineering, NLPKE, Tokushima, Japan.

[23] Kalempa, Vivian C. (2009) "Especificando Privacidade em Ambientes de Computação Ubíqua"; In UFSC, Dissertação de Mestrado, 140 pag. Access in: http://www.inf.ufsc.br/~bosco/ensino/ine6406/UbiComp/dissertacao_vivian.pdf - Acess in Nov 2017.

[24] Ros, M., D’Souza, M., Postula, A., MacColl, I. (2011) “Wireless outdoor personal area network using adaptive inquiry scanning for location-based services”. Personal and ubiquitous computing, v. 17, n. 2, p. 387-398. https://doi.org/10.1007/s00779-011-0501-2

[25] Afshan Samania, Hamada H. Ghenniwa, Abdul mutalib Wahaishi. PRIVACY AWARE SMART OBJECTS IN INTERNET OF THINGS in: Journal of Ubiquitous Systems and Pervasive Networks Volume 6, No. 2 (2015) pp. 01-10 DOI: 10.5383/JUSPN.06.02.001.

[26] Leithardt, Valderi R. Q., Guilherme Antonio Borges, Anubis Graciela de Morais Rossetto, Carlos Oberdan Rolim, Claudio Fernando Resin Geyer, Luiz Henrique Andrade Correia, David Nunes and Jorge Sa Silva: A Privacy Taxonomy for the Management of Ubiquitous Environments. Journal of Communication and Computer Volume 10, Number 12, December 2013 ISSN:1548-7709.

[27] Leithardt, Valderi R. Q., David Nunes, Anubis G. M. Rossetto Carlos O. Rolim, Cláudio F. R. Geyer, Jorge Sá Silva. Privacy Management Solution in Ubiquitous Environments Using Percontrol in Journal of Ubiquitous Systems and Pervasive Networks Volume 5, No. 2 (2014) pp. 21-28 DOI: 10.5383/JUSPN.05.02.004