

A Contextual Annotation-based Access Control Model for Pervasive Environments

José Bringel Filho^{*}
Joseph Fourier University,
Grenoble (FR)
LIG Laboratory, UMR 5217
681, rue de la Passerelle
Bringel@imag.fr

Jérôme Gensel
Pierre Mendès France
University, Grenoble (FR)
LIG Laboratory, UMR 5217
681, rue de la Passerelle
Jerome.Gensel@imag.fr

Windson Viana
Federal University of Ceará,
Fortaleza (BR)
Great Laboratory
Av. Mister Hull, s/n - Campus
do Pici
Windson@great.ufc.br

Hervé Martin
Joseph Fourier University,
Grenoble (FR)
LIG Laboratory, UMR 5217
681, rue de la Passerelle
Herve.Martin@imag.fr

ABSTRACT

With the growing interest in personal content managed by pervasive devices, such as photos, videos, and micro blog, important issues arise from the access control point of view. These sensor-rich devices offer users opportunities for creating, accessing, and sharing content from anywhere and at anytime, interacting dynamically with other surrounding devices and users. In this scenario, users and contents could be automatically annotated with information characterizing their situations (e.g., location, time, nearby devices) at request and creation time, respectively, which might interfere directly with the access permissions granted on protected content. This paper proposes a flexible and user-centric access control model for pervasive environments that explores contextual annotations in order to describe security policies and make access control decisions.

Categories and Subject Descriptors

K.6.5 [Management of Computing and Information Systems]: Security and Protection; H.3.4 [Systems and Software]: Distributed systems

General Terms

Security, Distributed systems

Keywords

Access control, pervasive computing, context-based decisions

1. INTRODUCTION

Subject to a constant improvement, sensor-rich pervasive devices are becoming powerful tools for content management. These devices offer users the support for creating, visualizing, retrieving, and sharing content, such as photos,

^{*}Supported by the Programme ALBan, the European Union Programme of High Level Scholarships for Latin America, scholarship no. E06D104158BR.

videos, audios, and micro blog. Moreover, it is now possible to use several sensors embedded on pervasive devices (e.g., GPS, Bluetooth, temperature, luminosity, accelerometer) for automatically creating annotations attached to the content [22, 21]. These annotations can be used to characterize the situation of content creation, namely contextual annotation, such as location, Bluetooth address of nearby pervasive devices, user activity, time, etc. Based on Dey's definition of context [4], we define contextual annotation as *any annotation that can be used to characterize the current or past situation of an entity. An entity is a person, place, or content that is considered relevant to the interaction between a user and an application, including the user and applications themselves.*

Nowadays, annotation is a common mechanism used by Web 2.0 platforms for attaching information to shared resources, mainly for the purpose of facilitating the retrieval of content or just as additional information about the annotated content. Services like Flickr¹ and Photomap² offer users the possibility to associate manually and semi-automatically tag-based annotations with photos that could be used for improving the retrieval, organization, and sharing operations.

However, existing annotation systems [21, 10, 19] do not exploit annotations as means of describing access control policies for protecting the annotated content. For instance, using these systems, it is not possible to describe access policies like "I grant read access on PhotoCollection1 only to my friends who were around when I took those photos." Or, "when I am in Paris, I grant read access on taken photos in this town only to my family." Existing access control models, such as MAC (Mandatory Access Control Model) [1], RBAC (Role-Based Access Control Model) [18], and extended RBAC models [15, 12, 3, 11], do not support this kind of access policies, since they were initially specified for closed and relatively unchangeable distributed systems, which deal only with a set of known users associated with roles grant-

¹<http://www.flickr.com/>

²<https://photomap.liglab.fr/PhotoMap/>

ing access permissions on a set of known services/resources. Furthermore, they do not take into account contextual annotations that describe the situation of content owners, requestors, and contents, when determining whether access should be given or not to the users [6].

We are mainly motivated by the need to extend these existing access control models towards the support of contextual annotations associated with the content, content requestor, and content owner, that could be used for defining access policies. To our knowledge, none of existing work takes into account these contextual annotation dimensions together in order to make access control decisions.

In this paper, we propose an access control model that generalizes the use of contextual annotation in order to address access control requirements in pervasive environments. This access control model is implemented using semantic Web technologies, such ontologies³ and inference/derivation rules⁴.

The remainder of the paper is organized as follows: Section 2 describes the proposed access control model. Then, we introduce a case study in Section 3. Section 4 presents related work and, in Section 5, we present some conclusion and future work.

2. A CONTEXTUAL ANNOTATION-BASED ACCESS CONTROL MODEL

Existing annotation systems like Annotea [10] and Vannotea [19], enable users to attach personal notes, questions, explanations, etc., to some content that can be categorized according to the media types, such as text, web pages, images, audio or video, 3D. Annotations vary from simple semantic tags to rich, structured annotations such as free text, hyperlinks, wikipedia⁵ entries, ranking, language, audiovisual, etc. These annotations can be attached to the fine-grained segments or regions of the annotated contents. In our approach, however, we are more interested in a subset of annotations that can be automatically sensed from the environment (e.g., GPS coordinates) or manually added by users for describing the context of users (content requestor and content owners) and contents, namely contextual annotation.

The proposed access control model is completely based on contextual annotations, where users are able to annotate manually their contacts (i.e. social network) and their contents (e.g. tags). This model offer users the possibility of defining access policies to describe *Who* can access *What* in which *Situation* (i.e., how, when, where, etc).

We consider that any content created by means of pervasive devices is automatically associated with raw contextual annotation describing the situation of creation (e.g., location, time, Bluetooth addresses of nearby devices). These raw contextual annotations can be used later by inference and derivation processes in order to have high-level contextual annotation. Users are also automatically annotated with information that describes their contexts at request time. Finally, content owners are able to define policies for granting access to their resources based on these annotations.

³<http://www.w3.org/TR/owl-features/>

⁴<http://www.w3.org/Submission/SWRL/>

⁵<http://www.wikipedia.org/>

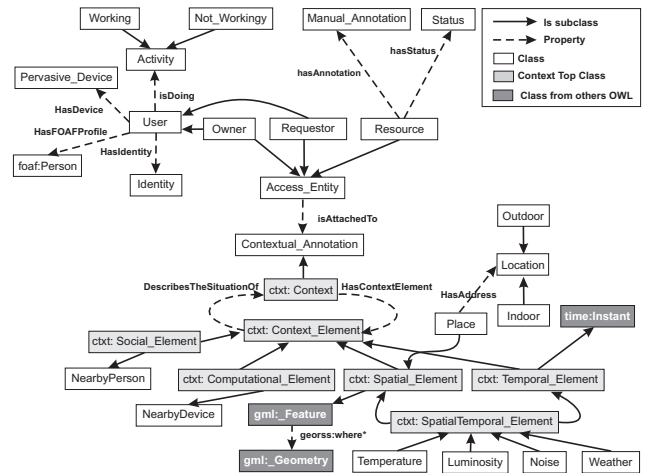


Figure 1: Contextual Annotation Ontology.

2.1 Contextual Annotation Model

It is necessary to define a formal contextual annotation model in order to facilitate the annotation representation, sharing, and semantic interoperability in the access control frameworks implementing the proposed model. For this purpose, we have defined an OWL DL ontology for modeling contextual annotation that can be used for defining access control policies. Our experience shows that using ontologies for context modeling is well suited for pervasive applications and services.

Based on our definition of *access entity* described in [7] that refers to any implicated element of an access control system (i.e., content owner, content requestor, and resource), we are classifying the contextual annotation related with each *access entity* according to five dimensions we consider as relevant for annotating and making access control decisions (see Figure 1): *spatial* - any information characterizing a situation in space (e.g., location, place, GPS coordinates); *temporal* - any information characterizing a situation in time (e.g., timestamp, period of day, month, year, day, season); *spatio-temporal* - any information characterizing a situation that depends on both spatial and temporal dimensions, i.e., each piece of information is associated with a particular location at a particular time (e.g., weather conditions, temperature, noise, luminosity); *social* - any information characterizing a situation using social relationships (e.g., nearby persons and nearby friends⁶); and *computational* - any information that describes a situation through computational characteristics (e.g., user's device capacities).

We have proposed in previous work the *Context top Ontology* [22, 21] for modeling the context dimensions listed above. We are reusing this ontology and the *Access Context Ontology*⁷ [7] as a basis for defining our contextual annotation model (see Figure 1). From the *Context* concept described in the *Context Top Ontology*, we have defined a subclass named *Contextual Annotation* (i.e., *Contextual_*

⁶By nearby persons or nearby friends we mean the social relationships associated with situation that the system is able to infer from Bluetooth addresses of nearby user's mobile devices.

⁷<http://membres-liglab.imag.fr/bringel/AccessContext.owl>

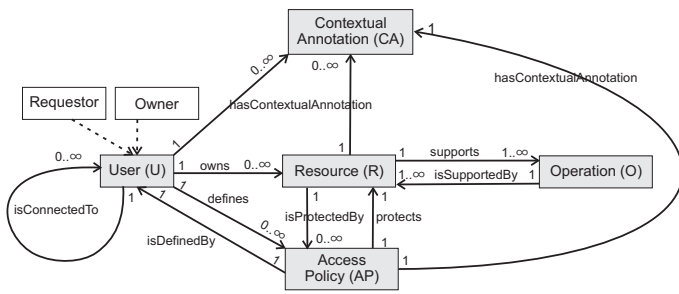


Figure 2: Main elements of the contextual annotation-based access control model.

Annotation \subseteq *Context*). This concept capture from the context any information that characterizes any *access entities* (i.e., content owner, content requestor, and resource) in which is relevant for making access control decisions. FOAF⁸ ontology has been extended in order to define new subclasses for classifying the social relationships existing between content owners and content requestors (e.g., family member, friend, bestFriend, supervisor, team member, etc). See in [7] for more details.

2.2 The proposed Access Control Model

The specification of the proposed model is based on RBAC [18] specification, but we are using the *Contextual Annotation* concept defined in the *Contextual Annotation Ontology* that represents any contextual annotation concepts relevant for taking access control decisions, instead of roles which is the main difference. Therefore, permissions are assigned to users (content requestor) taking into account *contextual annotations* that active some access control policies defined by content owners.

In fact, access policies defined using *contextual annotations* act as a mediator between users requiring access to contents and permissions assigned to these contents. Access control policies defined by content owners describe the contextual annotation conditions that must be satisfied in order to grant permissions on protected content.

This model is composed of five elements and relationships between them: User(U) (i.e., content owner and content requestor), Contextual Annotation (CA), Resources(R), Operations(O), and Access Policy (P). Figure 2 shows the proposed access control model and the relationships between them.

A *User* is connected to zero or more other *Users* by means of social relationships (e.g., FOAF profiles), and a *User* owns zero or more *Resources*. A *User* is able to define zero or more *AccessPolicies*. An *Contextual_Annotation* is a concept or a set of concepts (e.g., from the Contextual Annotation Ontology) that are connected together and aims to describe the *User* and the *Resource*. Each connection between *Users* can be annotated with zero or more *Contextual_Annotations* (e.g., Friend and teamMember).

A *Resource* is an entity owned by (*isOwnedBy*) one *User*. Each *operation* (e.g., read, write) can be associated with many *Resources*, and for each *Resource* can be granted many *Operations*. *Resources* are in the form of URIs and have zero or more *Access_Policies*. A *Access_Policy* is an

⁸<http://xmlns.com/foaf/spec/>

entity defined by (*isDefinedBy*) one *User* and protects (*protects*) one *Resource*. A *Policy* has one *Contextual_Annotation* that aims to describe the *User* and the *Resource* that should be shared with.

There exist several non-functional requirements for the proposed model:

- Only resource owners are able to define *access_policies* for protecting their resources, i.e., it is a user-centric access control model;
- A *user* obtains access to a resource, if and only if there exist a *access_policy* protecting that *resource* and the *contextual_annotation* at request time meets the *contextual_annotation* constraints described in that *access_policy*;
- If a *user* obtains access to a *resource* and she copies that *resource* to her *resources*, she will be a resource owner of that *resource*. The original resource owner will also keep the ownership as well;
- Support for sensing and management of contextual annotation associated with requestors and owners that should be available to access control framework implementing this model for making access control decisions;
- Support for sensing contextual annotation at creation time of resources, providing mechanisms to assist users in the task of context annotation of resources;
- It is required to guarantee security, privacy, and quality of contextual annotation used for making access control decisions, as we have identified in [5]. Compromised contextual annotation could cause incorrect access control decisions, resulting in security breaches on the access control system;
- In addition to determining contextual annotation at request time of protected resources and deciding whether to grant/deny access permissions, it should be possible to suspend a permission assigned to current contextual annotation when it changes to a state where the access conditions is no more true [23].

2.3 Defining and Enforcing Access Policies

We are using as a basis the ECA model (Event-Condition-Action) [2] for describing and enforcing contextual annotation-based access policies. In an access policy, the *Event* represents the identification of any changes on context. We are using our context management system proposed in [7, 8] for gathering contextual annotation we need to make access control decisions. Moreover, this context management system is in charge of protecting user's privacy requirements on her context information, by using an ontology-based approach.

Condition describes a set of valid contextual annotation constraints, and *Action* describes permissions that will be granted if the *condition* is true for the current contextual annotation. Our idea is to offer users a set of situations that they can use to define access policies for sharing their contents. Actually, we are carrying out research to identify the set of relevant contextual annotation dimensions and the more frequent set of sharing situations from the user's point of view, in order to propose a predefined set of access policy templates. Figure 3 shows the ECA schema for enforcing

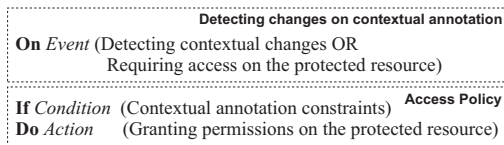


Figure 3: ECA schema for describing access control policies.

```

context rule := (' facts ' ) conditions '->' grant
facts := 'User(?user)' { '^ Grant(operation) } { [fact] }
fact := { '^ ( 'DataProperty |
           ObjectProperty |
           Individuals ' ) } /* Contextual Annotation */
conditions := { '^ ( 'atom' ) } /* Atom includes SWRL expressions */
operation := 'read' | 'write'
grant := 'hasAccess (?person, true)'
        { '^ hasAccessOf(?person, operation)' }

```

Figure 4: A part of the grammar EBNF of contextual access rules.

access control policies. When an access control framework that implements the proposed model receives an access request, it evaluates the contextual annotation associated with the content requestor, the content owner, and the requested content in order to grant/deny access on the protected content. There exist several ways to represent ECA rules. We are using a representation based on inference rules that is able to exploit directly semantic meta-data described using the *Contextual Annotation* ontology. We are using the language SWRL⁹ in order to explore the mathematical functions for expressing comparison (=) and inequality (> and <) between data properties that are useful expressions for describing conditions on access policies. We have adapted the contextual rule approach we proposed in [16] for enforcing access control policies. In this approach, the antecedent of an inference rule contains *facts* (i.e., gathered contextual annotations) and the activation conditions (i.e., context constraints) of an action that refer those *facts*. The resultant is an operation (e.g., read, write) on the protected resource that the system should grant to the content requestor. Therefore, in our approach:

- *Facts* are represented by contextual annotation meta-data of protected content;
- Context constraints describe the valid contextual annotation;
- The resultant adds relations to grant access on resource.

Figure 4 shows a part of the grammar EBNF (Extended Backus-Naur Form) of contextual access rules. Rules has a variable indicating users of social network (*User(?User)*) and operations on resource available in the system (e.g., read, write). Then, attributes of contextual annotation meta-data are listed. It may be optional in the access rule, since inference engines provide other forms of fact injection (fact), such as a simple indication of an OWL document. Contextual conditions may make reference to social, computational,

⁹<http://www.w3.org/Submission/SWRL/>

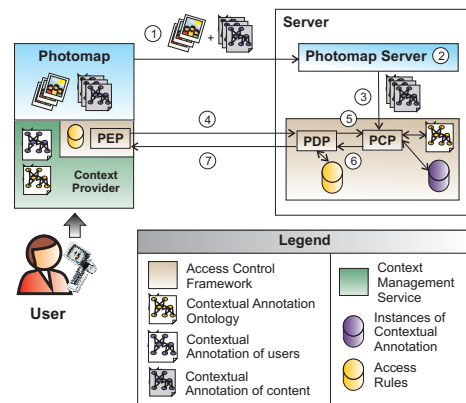


Figure 5: Overview of Photomap Application built on Our Access Control Framework.

spatial, temporal, and spatio-temporal data described by a instance of *ContextualAnnotation* Ontology. After executing contextual access rules the access decisions will be taken, granting or denying access on the protected resource.

3. CASE STUDY

We have evaluated our model to control access permissions on photos taken using the Photomap Application (see more detail in [22, 21]). In the Photomap application, photos taken by means of pervasive devices are automatically annotated with contextual information that describes the situation of users at photo shot time, such as location (GPS coordinates and the real address derived by Georeverse Web services), time, and Bluetooth addresses of nearby devices that are used for deriving the social context annotation. Then, this initial set of raw contextual annotation will be explored by inference and derivation processes executed on server-side in order to have new high-level contextual annotation, such as user's friends present at photo shot time, weather condition, temperature, etc.

Figure 5 illustrates a overview of Photomap application built on our access control framework that implements the proposed model. This framework follows a client-server architecture. The main components of our access control framework is based on XACML¹⁰ entities, such as PEP (Policy Enforcement Point) and PDP (Policy Decision Point) components that are in charge of querying and enforcing process of access rules, respectively (see in [7] for more details). Pervasive devices should deploy a client module in charge of: running contextual annotation functionalities (i.e., capturing contextual information and associating it to users and contents); describing access control policies by using predefined templates of access rules; requiring access on protected resources. Photomap client should send to the server-side Photomap application the user's access rules and the protected resources annotated with context information (1). Then, Photomap server executes (2) inference and derivation processes on contextual annotation associated with the photos, sending (3) these enriched documents to the PCP (Policy Context Information Point) that will update the base of

¹⁰http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

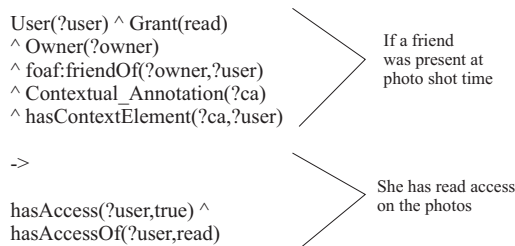


Figure 6: Example of access rule.

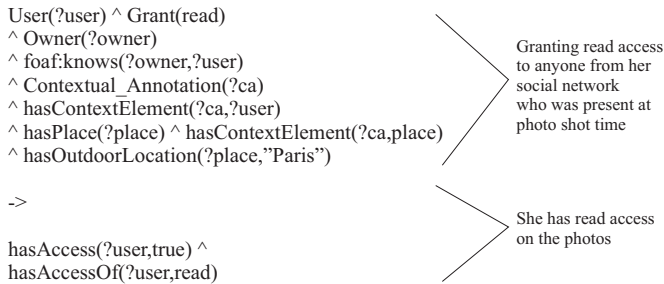


Figure 7: Example of access rule.

contextual annotation instances. Moreover, the client module should continuously send to the server context information associated with the user, i.e., a instance of *Contextual Annotation* ontology.

When a user try to access a protected content, PEP (4) requests access permission on that content to PDP. Then, PDP requests (5,6) to PCP the contextual annotation associated with the requested content, the current requestor, and the content owner. On receiving this contextual information set, PDP enforces the affected access rules (i.e., rules that protects the requested content), making annotation-based access control decisions. Finally, PDP grants/denies access (7) to the content requestor.

Using the Photomap client application, users are able to define access control policies for protecting their photos. For instance, a Photomap user intends to grant read access on her photos to users annotated as Friend who were present when the photo was taken. Figure 6 shows the contextual access rule that grants this permission to these users. In this case, each user who is annotated as Friend will have access to the URI of the taken photos.

Figure 7 shows a more elaborated contextual annotation-based access policy. In this case, the content owner intends to grant read access on her photos taken in Paris with anyone from her social network who were present at photo shot time.

4. DISCUSSION AND RELATED WORK

There are some approaches to control access based on annotations. In [19] is proposed the Vannotea system, an application designed to enable collaborating groups to discuss and annotate collections of high quality (images, video, audio or 3D objects), offering security mechanisms (authentication, and access control) for sharing these annotations with teams of trusted colleagues within a research or academic environment. The access, retrieval and re-use of an-

notation is controlled via Shibboleth¹¹ identity management and XACML¹² access policies. However, the authors are more interested in protecting the annotation information, which is different from our objectives (i.e., using annotation for defining access policies in order to protect the annotated content).

In [14, 13], Nasirifard *et al.* present an Annotation-Based Access Control model supported by a Collaboration Vocabulary (CoVoc) as a more flexible access control approach in social platforms and shared workspaces. The approach benefits from user annotations to annotate people using various fixed and desired open vocabulary (tags) and helps to build an access control mechanism based on relationships among different types of users. In summary, this approach allows the users to define her own annotations and assigns them to her contacts which is more user-centric. However, this approach makes access control decisions only based on annotations describing the social relationships between users (e.g., Friends, Collaborator). It do not take into account contextual annotation describing the situations of users (content owner and content requestor) and annotated contents.

Some research [3, 12, 17, 24, 11] attempts have been done in context-aware access control models, which take into account context information as an optional attribute used for limiting the scope of access control policies. Bertino *et al.* [3] have proposed the Temporal Role-Based Access Control Model (TRBAC) to add up the time dimension and the concept of role enabling/disabling in order to improve the RBAC model. Ray *et al.* [17] have extended RBAC towards a Spatial-Temporal Role-Based Access Control Model for taking into account both spatial and temporal context dimensions. Moyer *et al.* [12] have presented a Generalized Role-Based Access Control model (GRBAC), which extend the context dimensions supported by incorporating the notion of object roles and environment roles into RBAC model. Zhang *et al.* [24] have proposed the Dynamic Access Control Model (DRBAC) in order to deal with context information and Kim *et al.* [11] have proposed a similar approach that extends the RBAC model for adjusting dynamically role assignments (UA) and permission assignments (PA).

Some researches [23, 9, 20] have proposed context-based access control models, which permissions are assigned to users based on the current situation. Yokoyama *et al.* [23] have proposed an Anonymous Context Aware Access Control Architecture (ACA2) based on an analogy to the public telephone service, where users can anonymously access services supported by their context through pre-registered software components (proxies). Since this solution is focusing on architecture, no detail is given about the proposed access control model. Groba *et al.* [9] have presented a context-dependent access control for context information, which can be characterized by three basic properties: owner-centric, context-dependent, and individual role model for each user. However, this solution has been proposed to control access exclusively based on context information.

To the best of our knowledge, the work closest to our proposition is presented in [14, 13]. However, we have extended the support for annotating contents and users that can be used to define security policies and make access control decisions. In our access control model, access policies

¹¹<http://shibboleth.internet2.edu/>

¹²<http://sunxacml.sourceforge.net/>

can be described using any contextual annotation concept (e.g., location, time, social network, etc) that characterize the situation of content owner, content requestor, and content.

5. CONCLUSIONS

This work presents an access control model for pervasive environments that explores contextual annotations to define security policies and make access control decisions on annotated contents (i.e., the protected resource). Open, dynamic, and heterogeneous pervasive environments require new access control solutions, changing the focus of access control models from identity/role-based to the contextual-based approaches.

Some contextual annotation can be attached to users (content owners and content requestors) and contents, extending the existing annotation-based access control approaches. Content owners are able to define access policies based on contextual annotation attached to the content requestors, to their contents, and to them. According to our knowledge, none of existing annotation-based access control approaches for pervasive environments consider this kind of annotation for making access control decisions.

We have used semantic technologies (ontologies, SWRL rules) for describing and enforcing contextual annotation-based access control policies. We are currently working on implementing a prototype that integrates this model into Photomap Application [22, 21], in order to protect multimedia documents.

Moreover, we plan to extend the proposed model in order to take into account privacy requirements when enforcing access control policies. In addition, we plan to integrate a mechanism to dynamically and statically detect and resolve conflict on access control policies.

6. REFERENCES

- [1] Trusted computer system evaluation criteria, dod 5200.28-std, department of defense, 1985.
- [2] J. Bailey, A. Poulovassilis, and P. T. Wood. An event-condition-action language for xml. In *WWW '02*, pages 486–495, New York, NY, USA, 2002. ACM.
- [3] E. Bertino, P. A. Bonatti, and E. Ferrari. Trbac: a temporal role-based access control model. In *ACM Workshop on RBAC*, pages 21–30, 2000.
- [4] A. K. Dey. Understanding and using context. *Personal and Ubiquitous Computing*, 5(1):4–7, 2001.
- [5] J. B. Filho and H. Martin. Qacbac: an owner-centric qoc-aware context-based access control model for pervasive environments. In *SPRINGL '08*, pages 30–38, New York, NY, USA, 2008. ACM.
- [6] J. B. Filho and H. Martin. Using context quality indicators for improving context-based access control in pervasive environments. *EUC, IEEE/IFIP International Conference on*, 2:285–290, 2008.
- [7] J. B. Filho and H. Martin. A generalized context-based access control model for pervasive environments. In *SPRINGL '09*, pages 12–21, 2009.
- [8] J. B. Filho, A. D. Miron, I. Satoh, J. Gensel, and H. Martin. Modeling and measuring quality of context information in pervasive environments. In *AINA*, 2010.
- [9] C. Groba, S. Grob, and T. Springer. Context-dependent access control for contextual information. In *ARES '07*, pages 155–161, Washington, DC, USA, 2007. IEEE Computer Society.
- [10] J. Kahan and M.-R. Koivunen. Annotate: an open rdf infrastructure for shared web annotations. In *WWW '01*, pages 623–632, New York, NY, USA, 2001. ACM.
- [11] Y.-G. Kim, C.-J. Moon, D. Jeong, J.-O. Lee, C.-Y. Song, and D.-K. Baik. Context-aware access control mechanism for ubiquitous applications. In *AWIC*, volume 3528 of *Lecture Notes in Computer Science*, pages 236–242. Springer, 2005.
- [12] M. J. Moyer and M. Ahamad. Generalized role-based access control. In *ICDCS*, pages 391–398, 2001.
- [13] P. Nasirifard and V. Peristeras. Uncle-share: Annotation-based access control for cooperative and social systems. In *OTM '08*, pages 1122–1130, Berlin, Heidelberg, 2008. Springer-Verlag.
- [14] P. Nasirifard, V. Peristeras, and S. Decker. An annotation-based access control model and tools for collaborative information spaces. In *WSKS '08*, pages 51–60, Berlin, Heidelberg, 2008. Springer-Verlag.
- [15] S.-H. Park, Y.-J. Han, and T.-M. Chung. Context-role based access control for context-aware application. In *HPCC 2006, Munich, Germany, September 13-15, 2006*, volume 4208 of *Lecture Notes in Computer Science*, pages 572–580. Springer, 2006.
- [16] A. C. Ramos, M. Villanova-Oliver, J. Gensel, and H. Martin. Contextual user profile for adapting information in nomadic environments. In *WISE Workshops*, volume 4832 of *Lecture Notes in Computer Science*, pages 337–349. Springer, 2007.
- [17] I. Ray and M. Toahchoodee. A spatio-temporal role-based access control model. In *21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security, Redondo Beach, CA, USA, July 8-11, 2007*, volume 4602 of *Lecture Notes in Computer Science*, pages 211–226. Springer, 2007.
- [18] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. Role-based access control models. *IEEE Computer*, 29(2):38–47, 1996.
- [19] R. Schroeter, J. Hunter, J. Guerin, I. Khan, and M. Henderson. A synchronous multimedia annotation system for secure laboratories. In *E-SCIENCE '06*, page 41, 2006.
- [20] A. Toninelli, R. Montanari, L. Kagal, and O. Lassila. A semantic context-aware access control framework for secure collaborations in pervasive computing environments. In *International Semantic Web Conference*, pages 473–486, 2006.
- [21] W. Viana, J. B. Filho, J. Gensel, M. Villanova-Oliver, and H. Martin. Photomap - automatic spatiotemporal annotation for mobile photos. In *W2GIS 2007, Cardiff, UK, November 28-29, 2007*, pages 187–201, 2007.
- [22] W. Viana, J. B. Filho, J. Gensel, M. Villanova-Oliver, and H. Martin. A semantic approach and a web tool for contextual annotation of photos using camera phones. In *WISE*, pages 225–236, 2007.
- [23] S. Yokoyama, E. Kamioka, and S. Yamada. An anonymous context aware access control architecture for ubiquitous services. In *MDM2006, Nara, Japan, May 9-13, 2006*, page 74. IEEE, 2006.
- [24] G. Zhang and M. Parashar. Context-aware dynamic access control for pervasive computing, 2004.