

# Context-aware Access Control in Pervasive Healthcare

Wan-rong Jih<sup>1</sup>, Shao-you Cheng<sup>1</sup>, Jane Yung-jen Hsu<sup>1</sup>, Tse-Ming Tsai<sup>2</sup>

<sup>1</sup> Computer Science and Information Engineering, National Taiwan University, Taiwan  
*jih@agents.csie.ntu.edu.tw, {r93070, yjhsu}@csie.ntu.edu.tw*

<sup>2</sup> Advanced eCommerce Institute, Institute for Information Industry, Taiwan  
*eric@iii.org.tw*

## Abstract

*Progress in mobile devices, wireless networks and context-aware technologies are bringing pervasive healthcare into reality. With the help of wireless PDAs and portable computers, people may enjoy high quality care from a well-orchestrated team of healthcare professionals in the comfort of their own homes. The main technical challenges include mobility, adaptability, privacy, access authorization, and resource awareness. This paper presents a rule-based approach to context-aware access control in pervasive healthcare. The system is designed to work on resource-limited mobile devices over a peer-to-peer wireless network. Dynamic access authorization is achieved in real time by actively collecting context information, integrating the appropriate access control rules, and performing logical inference on the mobile device. Performance evaluations of the prototype implementation show the efficiency of the proposed mechanism.*

## 1. Introduction

Mobile devices over wireless networks enable new applications and services of *pervasive healthcare* [3, 4, 6, 9, 20]. For example, by utilizing lightweight PDAs or laptops, healthcare practitioners will be able to better communicate with the patients, and to access updated patient medical records anytime and anywhere. To provide quality and effective medical services, it is often necessary to share and exchange medical information among the healthcare practitioners caring for a specific patient.

Pervasive computing aims to expand mobility while providing services in a seamless fashion. To cope with changing configuration due to mobility of the user in

the environment, applications need to be context-aware and adaptive [17]. The term *context* refers to the information that one can retrieve from the current situation, such as where you are, who you are, and what objects are nearby [8]. Context-aware computing demands an infrastructure that adapts to real-time situation and brings the most appropriate information and services to the users, so they can focus on their main task. Several context-aware applications have been developed for the healthcare domain [1, 3, 9].

The United States federal government enacted the HIPAA (Health Insurance Portability and Accountability Act [14]) standards in 1996. The so-called *Privacy Rule* is intended to standardize the management of security, privacy and data exchange of personal medical information. To protect the privacy of individuals, HIPAA requires healthcare practitioners to obtain patient consent for disclosure of any protected health information (PHI) for authorized purposes.

The most important technical challenges in providing pervasive healthcare services include mobility, portability, access authorization, privacy and security [18]. As pervasive healthcare is often characterized by high degree of mobility but low level of infrastructural support [5, 12, 15, 16] (e.g. a patient's home), authorization and data access will be carried out on mobile devices with limited resources in real time. In addition, access control decisions may depend on the context, e.g. time, location, and the presence of certain conditions or individuals. To meet the challenges, a *ubiquitous care service platform* has been proposed in [19]. In particular, context-aware rule-based reasoning is employed to perform dynamic access control of PHI and other personal information. The rule engine can integrate the changing contexts into its knowledge base, and make access control decisions dynamically. The proposed context-aware access control mechanism operates on top of a peer-to-peer net-

work for efficient distribution and collaboration.

This paper proposed a rule-based approach to dynamic *context-aware access control* in pervasive healthcare. In the next section, we will illustrate the context-aware access control problem using an in-home healthcare scenario. Section 3 presents the proposed solution by describing the system architecture and the functions of individual components. Performance evaluation of running the rule engine on a mobile device is shown in Section 4, which also include sample screenshots to demonstrate the user interface of the implemented system. Finally, we summarize the contribution of this research in Section 5.

## 2. A Sample Healthcare Scenario

This section presents a sample in-home healthcare scenario to illustrate the context-aware access control problem. In general, a wide variety of data can be created and maintained for each patient. Given any specific healthcare situation, multiple medical professionals may be involved in the process. To support high quality medical care and better collaboration, healthcare practitioners use wireless mobile devices such as PDAs or tablet PCs to access data from a centralized server or to exchange information among themselves. Protecting, managing and sharing such medical data is an essential issue in pervasive healthcare.

### 2.1. Scenario

The following scenario describes a three-member multidisciplinary team delivering healthcare services at the patient's home during different time periods.

Peter was injured in an accident and suffered from depression. He has been under the care of Mark, a physiotherapist, and Philip, a psychiatrist. Alice, the community health advisor, is in charge of the multidisciplinary team to provide ongoing care and rehabilitation for Peter within a secure and therapeutic environment. Services of each medical professional can be performed in a hospital, a nursing home, or the patient's home.

In order to provide proper medical services, the healthcare team may share Peter's health information among its members under strict access control. Each medical professional usually maintains specialized medical records on the same patient. They may share the records among each other for improved treatment quality and effective medical services. On the other hand, patient medical information is private and should be protected. Prior authorization is often required for requests from other medical

professional to use or disclose any protected health information.

### 2.2. Scenes

A detailed scene-by-scene description of the sample scenario is given as follows.

Based on the medical privacy regulations issued by the United States Department of Health and Human Services in April 2003, physicians are required to keep two types of patient records. For example, a psychiatrist should maintain a separate set of psychotherapy notes (*i.e.* mental health records), which are notes analyzing or documenting the contents of conversation during a private counselling session, in addition to the regular medical records (*i.e.* basic information records). With proper authorization, patient health information may be used and shared for purposes of treatment in delivering quality and effective medical services.

In the sample scenario, data exchange is carried out by wireless devices communicating through a common access point. At 10:25 AM, Alice was authorized to access Peter's mental health records. Upon Philip's leaving Peter's home at 10:40 AM, access authorization expires at the end of the 15-minute extension. Consequently, Alice can use the mental health records till 10:55 AM. In contrast, access is revoked as soon as Mark leaves Peter's home.

### 2.3. Context

Dey and Abowd [7, 8] described: "Context is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves." Context can be defined as the information that contains location, identity, time and activity, and these information can be used to characterize the situation of a participant information while an interaction among these entities occurred. In addition, context may also include system capabilities, services, the activities and tasks in which people and computing entities are engaged, and their situational roles, beliefs, and intentions.

In the sample scenario, participants are the patient Peter, physiotherapist Mark, psychiatrist Philip and the community health advisor Alice. The medical services take place at Peter's home. Activities among the participants include sharing Peter's medical records with prior authorization, exchanging access control rules, maintaining coherent medical records, checking visitation history, and so on. The medical records, history logs and

**Table 1. Scenes from in-home healthcare.**

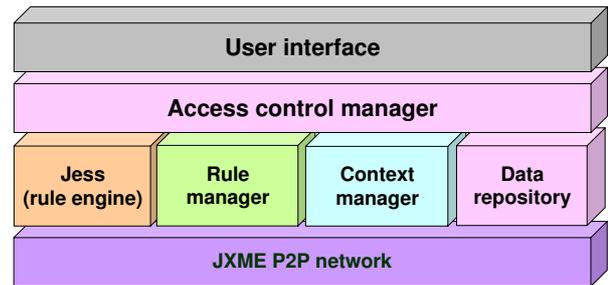
Time	Description
10:00 AM	<ul style="list-style-type: none"> <li>Psychiatrist Philip arrives at Peter's home.</li> <li>Philip retrieves Peter's basic information.</li> <li>Philip reviews Peter's mental health records, which are kept separately from the basic information.</li> </ul>
10:20 AM	<ul style="list-style-type: none"> <li>Alice arrives at Peter's home.</li> <li>Alice retrieves Peter's basic information.</li> </ul>
10:25 AM	<ul style="list-style-type: none"> <li>Alice discusses Peter's condition with Philip.</li> <li>Alice requests permission to view Peter's mental health records.</li> </ul>
10:30 AM	<ul style="list-style-type: none"> <li>Physiotherapist Mark arrives at Peter's home.</li> <li>Mark examines Peter's basic information.</li> <li>Mark uses the physiotherapy notes to evaluate Peter's physical condition.</li> </ul>
10:35 AM	<ul style="list-style-type: none"> <li>Alice chats with Mark while requesting permission to view Peter's physiotherapy notes.</li> </ul>
10:40 AM	<ul style="list-style-type: none"> <li>Philip updates Peter's <i>mental health records</i>.</li> <li>Phillip grants a fifteen-minute access authority to Alice.</li> <li>Philip leaves Peter's home.</li> </ul>
10:50 AM	<ul style="list-style-type: none"> <li>Mark updates Peter's physiotherapy notes.</li> <li>Mark leaves Peter's home.</li> <li>Alice can no longer access Peter's physiotherapy notes due to Mark's departure.</li> </ul>
10:55 AM	<ul style="list-style-type: none"> <li>The fifteen-minute access authorization expires.</li> <li>Alice can no longer access Peter's mental health records.</li> </ul>
11:00 AM	<ul style="list-style-type: none"> <li>Alice checks the medical professionals' visiting log.</li> </ul>
11:10 AM	<ul style="list-style-type: none"> <li>Alice wraps up her visit and leaves Peter's home.</li> </ul>

rules are apparently the computational objects. More detailed scenes will be given in next section.

Access control authorization should depend on the current context. To protect patient privacy information, no information should be shared without consent. Given the dynamic context that changes from scene to scene, access control decisions have to be made in real time. Access control rules should be collected dynamically in order to achieve accurate authorization result. In general, each medical professional should obtain authorization before he/she can access the personal privacy records.

### 3. Context-aware Access Control

We design an adaptive system for achieving the real-time, accurate and effective context-aware access control. Figure 1 is the system block diagram of our ap-



**Figure 1. System architecture**

proach, which will be running on every mobile device of the healthcare participant.

The top layer of our system provides user interface, and access control will be performed to inquiry the authorization results. Middle layer includes modules of rule engine, rule manager and context manager. These components would tightly cooperate and coordinate with each other. As a network layer, we adopt P2P infrastructure for supporting the requirements of communication – dynamic rule exchange, context gathering, real-time authorization, documents sharing, and so on.

In the following subsections, we will describe the key components of our system. A diagram will be shown in Section 3.4, for illustrating the interaction among systems.

### 3.1. Context manager

As the context might be changed at anytime, a context collector will detect ambient information. If the context has been changed, context manager should update the corresponding status and announce such variation to other managers. So far in our system, context change will trigger rule gathering and might affect the access authorizations. Figure 2 describe the flow of context manager.

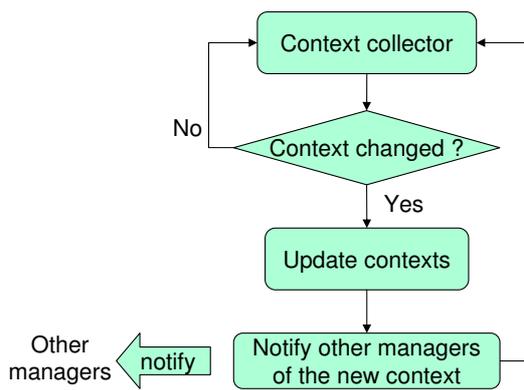


Figure 2. Context manager

According to the scenario of Section 2.2, context changes from scene to scene. For example, at 10:00 AM, while the psychiatrist Philip arrives Peter’s home, context associated with Philip will change, including Philip’s current location, how many participants in Peter’s home and their roles, current available documents for sharing, and so on. Meanwhile, context manager updates the participant list and informs access control manager to update available document list. In addition, an event of Philip’s arrival will be sent to rule manager.

### 3.2. Access control manager

Access control manager receives request from the user and will derive authorization result from rule manager. Actually, rule manager supports a simple query interface for such access requests. The permission outcome indeed are inferred by rule engine and will return to the claimer via P2P network.

Refer to the scene at 10:25 AM, Alice wants to access Peter’s mental health record, which belongs to the psychiatrist Philip. Alice’s access control manager will figure out that Alice does not have right to access this record, and owner of the record is Philip. In order to get the permission from Philip, Alice’s access control

manager will automatically send an access request to Philip’s PDA.

Consider the other side on Philip’s PDA, as system receives access request from Alice, access control manager dispatches this task to rule manager. Authorization result will be sent back to Alice’s access control manager after Philip’s rule engine finished reasoning. If Alice gets the permission to access the mental health record, meanwhile, the access control manger will send the up-to-date record to Alice.

Communication among different modules is using the JXTA-J2ME (JXME) network [2]. Deploy JXME network on mobile devices make the devices can participate to P2P activities with other devices. Consequently, peers of access control manager will communicate and collaborate in a P2P manner.

### 3.3. Rule manager

When rule manager receives a query, a rule engine Jess [11] is used to make an inference result. Jess is completely developed by Java language and uses Rete algorithm [10] to process rules, where the rules is compatible with CLIPS [13]. Rules contain information for determining whether a certain user can access the specified records or not. In our scenario, each healthcare participant will carry his/her own relevant privacy rules and merge them into knowledge base while inferring. Figure 3 depicts the control flow of rule manager.

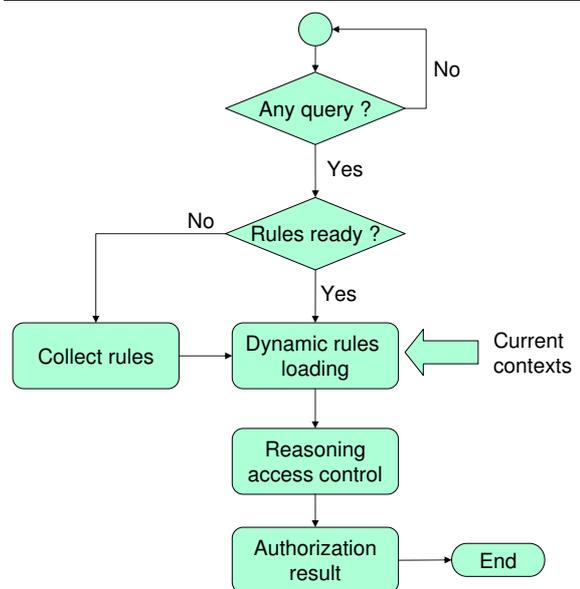


Figure 3. Rule manager

Contents of rule set is various and highly depends on the current context. Rule manager yields dynamic rule collection when environment has been changed; it automatically collects rules in order to provide more correct result and infers efficiently for the further requests. In our system, when rule manager receives a request, an appropriate rule set will be constructed in according to the participants of a specified location, and the rule engine infers the result subsequently.

### 3.4. Context-aware authorization

Figure 4 depicts the interaction among users, for obtaining the access permission of health records. Both Alice and Philip are using mobile device to keep patients' health records. The patient stays at a place (e.g. his home) with deployment of wireless network server. In our system, while these medical professionals carry their PDAs and deliver the health services to the patient, each context manager will detect current location and alert to the other managers. Access control manager would handle requests, and pass it to appropriate destinations, where rule manager maintains the consistency of rules and invokes rule reasoning.

## 4. Evaluation and Demonstration

Resources of mobile devices are limited, therefore, we present the performance evaluation of rule design. In addition, some screenshots have been used to demonstrate our context-aware access control system.

### 4.1. Evaluation

We adapt context-aware access control in pervasive environment, and utilize a rule-based system to provide real-time reasoning. As we know that mobile devices have scarce resources, such as low battery power, slow CPU and little memory. Unfortunately, rule interpretation and deduction are memory consumed and demand highly computing power to support dynamic context environment.

Figure 5 compares the rule loading time between desktop and PDA. Our experimental result shows that rule parsing and Rete tree constructing are time consumed. Apparently, PDAs suffer from increasing time cost while the rule size is grown.

The experiments have been done on a Pentium 4 at 2.6 GHz desktop with 1 GB RAM. In regarding the mobile device, we use an iPAQ H4150 PDA at 400 MHz processor with 64 MB RAM. For gaining fair and precise results, experiments are referred to the same rule set and knowledge base.

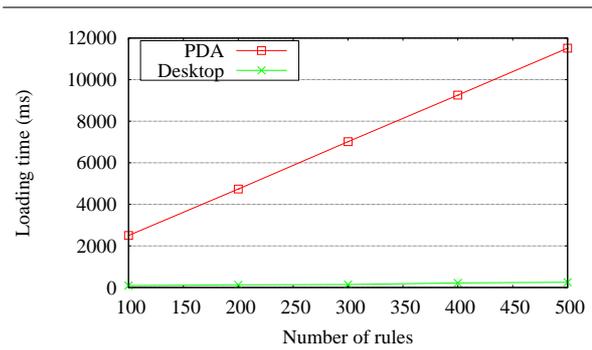


Figure 5. A comparison of rule loading time

Though Rete is an optimal pattern matching algorithm utilized by Jess, performance on limited memory devices is still a critical issue. From Figure 5, the loading time is proportional to the number of rules. Consequently, reduce the number of rules and facts will improve the performance. We suggest some guidelines for such improvement:

- *Completely and comprehensively understand domain knowledge will help rule design.*
- *Correctly and clearly identify context as dynamic facts in rules.*
- *Reorder patterns of each rule for minimizing partial matches.*

The first statement states the importance of domain knowledge. Different application domain requires different knowledge representation, like as rule expression, content of facts. Using proper terminology to present a fact, and minimized the number of fact, so that can save working memory size and speed up the inference time.

Rule designer has to concern the dynamic property of context, that is, context might change at any condition and can be referred as *dynamic* facts, in comparison with *static* facts. Distinguish context from facts and avoiding reload of static facts can decrease the response time. Because of reloading facts is time consumed and inefficient. Static facts are always remain constantly after they have been loaded into rule engine; whereas, dynamic facts might change all the time. Therefore, we recommend that only reload the dynamic facts if necessary.

Figure 6 describes an example of two rules. Rule rule-1 consists of two patterns, (location (where ?location)) contains a dynamic fact ?location and (person (name Alice) (role Advisor)) comprises two static facts. Reorder the patterns in a rule will change the Rete

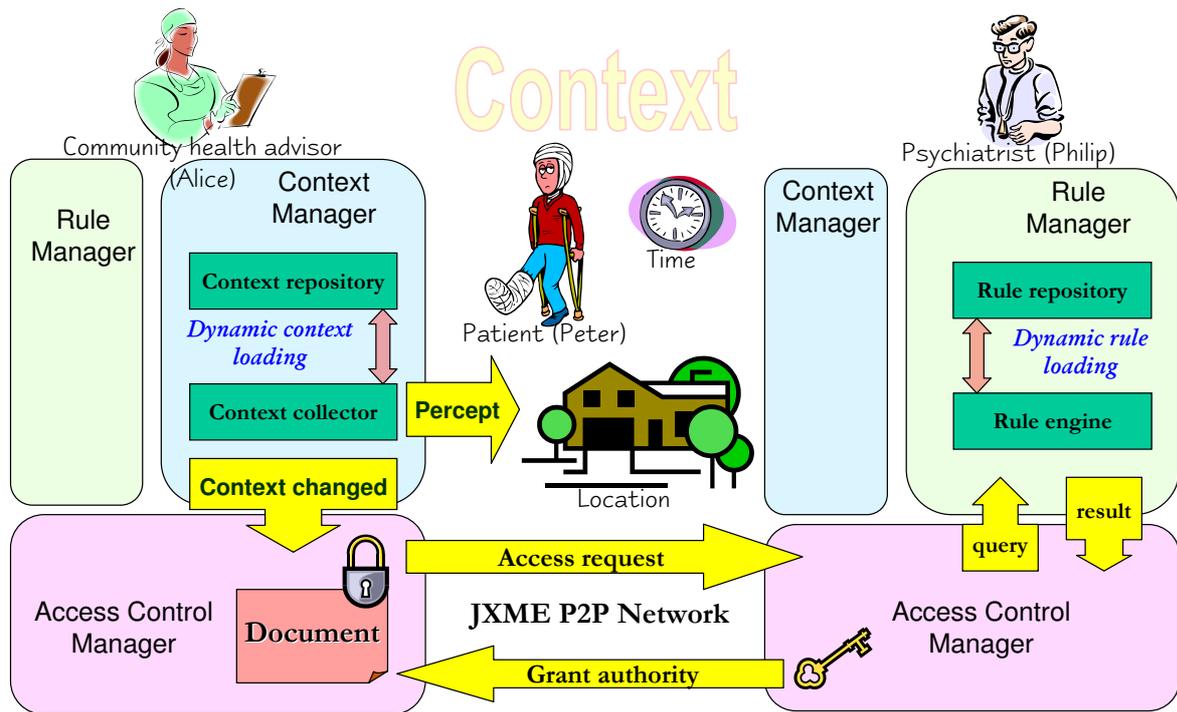


Figure 4. Modules interaction of context-aware access control

```

(defrule rule-1
  (location (where ?location))
  (person (name Alice)(role Advisor))
  ...
  =>
  ... )

(defrule rule-2
  (person (name Alice)(role Advisor))
  ...
  (location (where ?location))
  =>
  ... )

```

Figure 6. Rule examples

network, the upper nodes will be accessed more frequently due to the top-down matching behavior of algorithm. Consequently, rule-2 is more efficient than rule-1, because that pattern contains dynamic fact ?location is close to the bottom of rule's left hand side (LHS).

Pervasive healthcare involves distributed and collaborative environment, knowledge will contain large number of facts. Figure 7 shows pattern ordering certainly affects the performance of reasoning. Line with square points is the rule set without any optimized pattern re-

ordering, the other line close to the x-axis is the re-ordered rule set. If we do not refine rules, rule engine on PDA can merely match 30 facts. The refined rules do not have such handicapped.

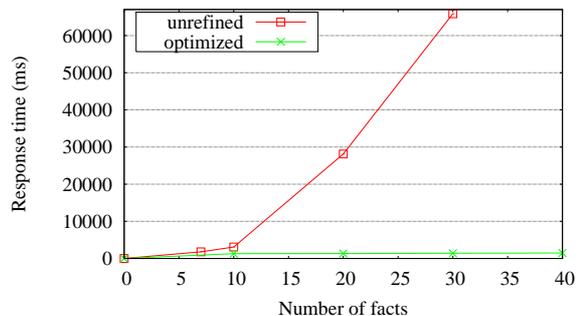


Figure 7. The impact of reorder patterns among same rule set

## 4.2. Demonstration

Following the scenes in Section 2.2, we selective demonstrate some typical activities screenshots. At



Figure 8. Screenshots captured from PDA emulator

10:20 AM, Alice arrives Peter's home, her PDA shows a login interface as Figure 8(a). At 10:25 AM, Alice wish to disclose Peter's mental health record and get access permission from Philip, Figure 8(b) is this document. At 10:55 AM, authorization limit is reached, Alice can not access the records from now on. Figure 8(c) shows this revocation.

## 5. Conclusion

Sharing privacy health information under a secured and authorized environment imposes an important technical challenge for realizing pervasive healthcare. Traditional rule engine does not deal with dynamic access control in a mobile computing environment. In this research, we explored the idea of rule-based merging to deal with dynamically changing contexts.

Given that the proposed context-aware rule engine runs on resource-limited mobile devices, performance becomes an important issue. In order to make the rule engine run smoothly and efficiently, we employ techniques for minimizing the number of rules and facts, and reordering the sequence of pattern matching. Following these rule optimization criteria, the rule engine is shown to produce query results in real time.

We plan to design more complex scenarios to conduct more comprehensive test and evaluation of our system. In general, the more participants are involved, the more complicated interactions will be. We also expect the size of knowledge base to grow significantly when the problem is more complex. Currently, pattern reordering is done manually, and it is desirable

to automate the optimization steps. Furthermore, other rule optimization techniques should be explored to improve performance on mobile device. Other important research issues include a better user interface on the mobile device, utilizing the visitation log for billing and diagnosis, and fine-grain access control.

## Acknowledgements

This research was supported by a grant (93-CS-1218) from the Advanced eCommerce Institute of the Institute for Information Industry (III) in Taiwan. Special thanks should go to Jiann-Tsuen Liu for hours of discussions and valuable suggestions on this project. The authors would like to thank other members of the Intelligent Agents Lab at National Taiwan University – Rong-che Lee, Ting-hsiang Huang, Chia-nan Ko, Chi-yau Lin, and Chia-en Tai, for their contributions to the prototype implementation.

## References

- [1] Centre for pervasive healthcare. <http://www.healthcare.pervasive.dk>, 2004. Aabogade 34, DK-8200 Aarhus N, DENMARK.
- [2] JXME: JXTA platform project, 2004.
- [3] J. E. Bardram. Applications of context-aware computing in hospital work: examples and design principles. In *Proceedings of the 2004 ACM symposium on Applied computing (SAC '04)*, pages 1574–1579. ACM Press, 2004.
- [4] J. E. Bardram, H. B. Christensen, and A. K. Olsen. Hypernavigation in the physical space: Adapting presenta-

- tions to the user and to the situational context. Technical report, Centre for Pervasive Computing, 2004.
- [5] H. B. Christensen. Using logic programming to detect activities in pervasive healthcare. In *Proceedings of 18th International Conference on Logic Programming (ICLP 2002)*, pages 421–436. Springer-Verlag, July 29-August 01 2002.
  - [6] H. B. Christensen and J. Bardram. Supporting human activities - exploring activity-centered computing. In *Proceedings of the 4th international conference on Ubiquitous Computing (UbiComp '02)*, pages 107–116. Springer-Verlag, 2002.
  - [7] A. K. Dey. Understanding and using context. *Personal Ubiquitous Computing*, 5(1):4–7, 2001.
  - [8] A. K. Dey and G. D. Abowd. Towards a better understanding of context and context-awareness. Technical Report GIT-GVU-99-22, Georgia Institute of Technology, College of Computing, June 1999.
  - [9] J. Favela, M. Rodriguez, A. Preciado, and V. M. Gonzalez. Integrating context-aware public displays into a mobile hospital information system. *Information Technology in Biomedicine, IEEE Transactions on*, 8(3):279–286, Sept. 2004.
  - [10] C. Forgy. Rete: A fast algorithm for the many patterns/many objects match problem. *Artificial Intelligence*, 19(1):17–37, 1982.
  - [11] E. Friedman-Hill. Jess, the rule engine for the java platform. Sandia National Laboratories, 2005.
  - [12] F. Gandon and N. M. Sadeh. A semantic e-wallet to reconcile privacy and context awareness. In *Proceedings of Second International Semantic Web Conference (ISWC 2003)*, pages 385–401, October 20-23 2003.
  - [13] Bruno Haible and Michael Stoll. CLIPS: ANSI common lisp standard. <http://clisp.cons.org/>, 2005. GNU Free Documentation License.
  - [14] HIPAA. Health insurance portability and accountability act. <http://www.hipaa.org/>, 1996.
  - [15] X. Jiang, N. Y. Chen, J. I. Hong, K. Wang, L. Takayama, and J. A. Landay. Siren: Context-aware computing for firefighting. In *Proceedings of Second International Conference on Pervasive Computing*, pages 87–105. Springer, April 18-23 2004.
  - [16] A. Ranganathan and R. H. Campbell. An infrastructure for context-awareness based on first order logic. *Personal Ubiquitous Computing*, 7(6):353–364, 2003.
  - [17] M. Satyanarayanan. Pervasive computing: Vision and challenges. *IEEE Personal Communications*, 8(1):10–17, August 2001.
  - [18] V. Stanford. Pervasive health care applications face tough security challenges. *IEEE Pervasive Computing*, 1(2):8–12, 2002.
  - [19] T. M. Tsai, J. T. Liu, and J. Y. J. Hsu. Micare: Context-aware authorization for integrated healthcare services. In *UbiHealth 2004: The 2nd International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications*, 2004.
  - [20] U. Varshney. Pervasive healthcare. *Computer*, 36(12):138–140, 2003.