A Study on Secure Contents Using in Intelligent Urban Computing

Hoon Ko[1], Jongmyung Choi[2], Maricel O. Balitanas[3],
Tai-hoon Kim[4] and Carlos Ramos[5]
*[1 5] GECAD, Institute of Engineering Polytechnic of Porto,
Rua Dr. Antonio Bernardino de Almeida, 431, 4200-072 Porto, Portugal.
[1] hko@isep.ipp.pt, [5] csr@dei.isep.ipp.pt
[2] Department of Computer Engineering, Mokpo National University,
61, Dorim-Li, Chyounggye-Myeun, Muan-Gun, Jeon-nam, S. Korea.
[2] choijm@gmail.com
[3, 4] Department of Multimedia Engineering, Hannam University,
Ojeong-dong, Daedeok-Gu, 133, 306-791, Daejeon, S. Korea.
[3] maricel@sersc.org, [4] taihoonn@empal.com*

Abstract

Ubiquitous computing only allows services of fixed or local area and it just provides services without status information of the device upon user request. Thus, it is difficult to react immediately with users changes. Since urban computing is on higher system instead of ubiquitous, it can usually provide users the organic behavior with reference from devices physical states information. Also, it provides the services by considering the user's devices and environments near user's location. That means the generated context during movement can be detected by sensor. Through this information the system guesses the user's next move and the number of context increases upon user's movement. Therefore, there are so many users / devices to attack in urban computing. However, existing urban computing is insufficiency to process the security module. Therefore, we suggest the way to secure contents in urban computing.

Keywords: *Urban Computing, Context-Aware, Contents, Spam-mail, Authentication / Authorization.*

1 Introduction

Ubiquitous computing presented at early 1990's, has been developed in various networks. It only allows services of fixed or local area and just provides services without status information of the device upon user's request. In other words, it means that direct operation to user changes is almost impossible. On the other hand, there is an urban computing, which is located higher than ubiquitous. The aim of urban computing is to continually provide services between users and space / environment information near moving users [3]. That is, users can take all services as they move over their devices through processing organic processing between user's environment and space environment. The relation among users, between users and urban constituent are very important in urban space. Because users usually ask useful services during their moving, also users would like to receive the services what they want from some shops without any stopping. Users periodically may want to get that information or during their shopping. These days, sending information to users are commonly done through SMS or letter. Although some company services have problems in dealing with user's request, problems like no detail of products, sending them to users who don't want to get, etc. However this kind of e-mail can be considered as SPAM in future. Anyway, in order to receive exact information of what they want to send; first users have to register asking information into shops (called CP, it's server in each shop). And contents provider (CP) must keep it up-to-date, a certificate Server (CS) and a secure server (SS) should control the security service between contents servers and users. Also, CS and SS have to observe attacks by attackers. If attackers illegally put his information to CP, users in database may receive unwanted information. To protect those problems, CS has to process an authentication to confirm integrity for their asking. This paper is totally composed of five chapters. Section 1 is an introduction and we describe the related works in section 2. We explain our proposed secure context processing in section 3; section 4 is the area for discussion. At last, we make a conclusion in section 5.

2 Related Works

2.1 Ambient Intelligence

Ambient Intelligence (AmI) concept was introduced in 2001 by ISTAG (European Commission's IST Advisory Group), and provides a vision of the Information Society where people are surrounded by intelligent intuitive interfaces that are embedded in all kinds of objects and an environment that is capable of recognizing and responding to the presence of different individuals in a seamless, unobtrusive and often invisible way [1]. In that sense AmI refers to a digital environment that proactively, but sensibly, assists people in their daily lives. We can find examples of Ambient Intelligent (AmI) applications in several environments: smart homes, smart offices, intelligent meeting rooms, ambient healthcare, smart classrooms [1][2]. These "intelligent" or "smart" environments and systems interact with human beings in a helpful, adaptive, active and unobtrusive way. These environments/systems may still be pro-active acting autonomously anticipating the user's needs, and in some circumstances they may even replace the user. AmI is closely related with areas like ubiquitous computing, pervasive computing, context awareness and embedded systems, but with distinctive differences [1]. Context-aware concept was introduced in 1994 by B. Schilit, N. Adams and R. Want, and was defined as software that adapts according to its location of use, the collection of nearby people and objects, as well as changes to those objects over time. A more recent definition is from Dey defines context aware software as systems that use context to provide relevant information and/or services to the user, where relevancy depends on the user's task. Chen and Kotz classified context in four categories: physical context, computing context, user context, and time context. Context information could be related to the actual moment or can be historical, i.e., when user, computing, physical and time context are stored along a time span. Historical context information can be very useful to establish patterns and predict some of the possible user's actions. However it must be carefully considered which historical information is worthy of being kept, and in which level of precision. Storing all the context information that is collected can make the process of evaluating that information very expensive [1].

2.2 Urban Computing

Ubiquitous computing has limitation to use information of place features, social and time means that urban space has, because ubiquitous computing only involves simple information services about user's location or about limited space [14]. For example, in case a living room, when there is only family there, they feel comfortable for rest, however if that room will be the space for public meeting, it can be public space at that time. Therefore, some people in living room may feel each way according to their purpose. In the same way, some people are in a park, some of them who go there to work is a work space, but to those who go there to take a walk will consider the space as rest area only. That is, one space can have different meaning depending on time flowing or people's purpose. Finally, it has to provide the optimized service to user after considering the social relation among users who are sharing the same space which has multiple meaning. Also, it has to be changed the security component dynamically depend on user's location and space features. However, ubiquitous computing, which considers only simple context has limitation to provide services in global space like urban space.

3 Secure Context Operating

3.1 Security Functions

We explain about each mission of four, which is a context allocator, a context analyzer, a context collector, and a context detector for secure processing in urban computing [Fig. 1] [4].

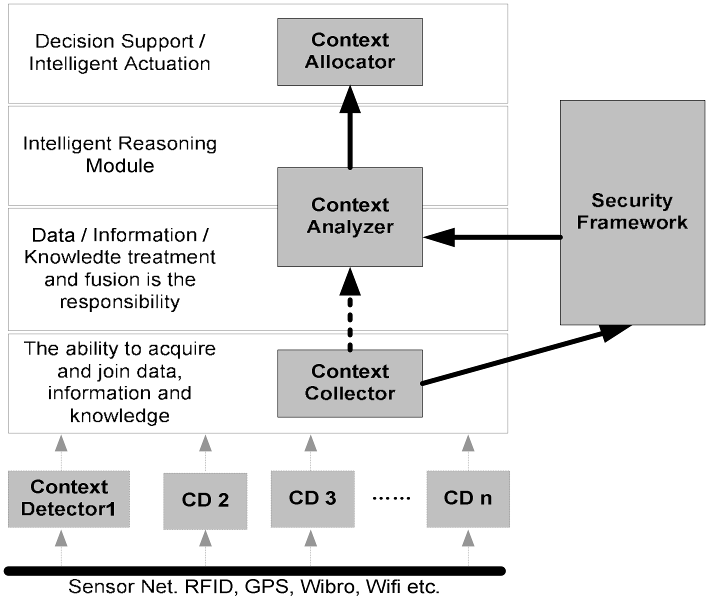
Decision Support / Intelligent Actuation
Context Allocator
Intelligent Reasoning Module
Context Analyzer
Security Framework
Data / Information / Knowledte treatment and fusion is the responsibility
The ability to acquire and join data, information and knowledge
Context Collector
Context Detector1
CD 2
CD 3
……
CD n
Sensor Net. RFID, GPS, Wibro, Wifi etc.

Fig. 1 Security Functions

Context Detector (CD): CD is to detecting to all contexts changing.
Context Collector (CC): CC gets together all contexts from CD. First processing of security (An authentication / an authorization) is this area's job. All contexts that were detected on all sensors will be transferred to security framework [4][9], and then they get a security processing. According to this process, they decide whether they set the security level or not.
Context Analyzer (CA): CA defines the security policy received context from CC.
Context Allocator (CoA): CoA suitably arranges them to each module.

3.2 Urban Life

User A and user B have to register their request for the information they wanted in the product before moving. Also, each shop has to keep their information of product up to date in CP [Fig. 2]. Therefore, CP is keeping some information which is user requesting item and registered product contents by shops, and then CP sends information to user device related with between tables in databases. Definition of each acronym is shown in table 1.

Table 1. Definition

Symbol	Name	Contents
C	Contents	detail information of all products
CS	Certificate Server	Control all SS / User
CP	Contents Provider	Support product information
SS	Secure Server	Control CPs

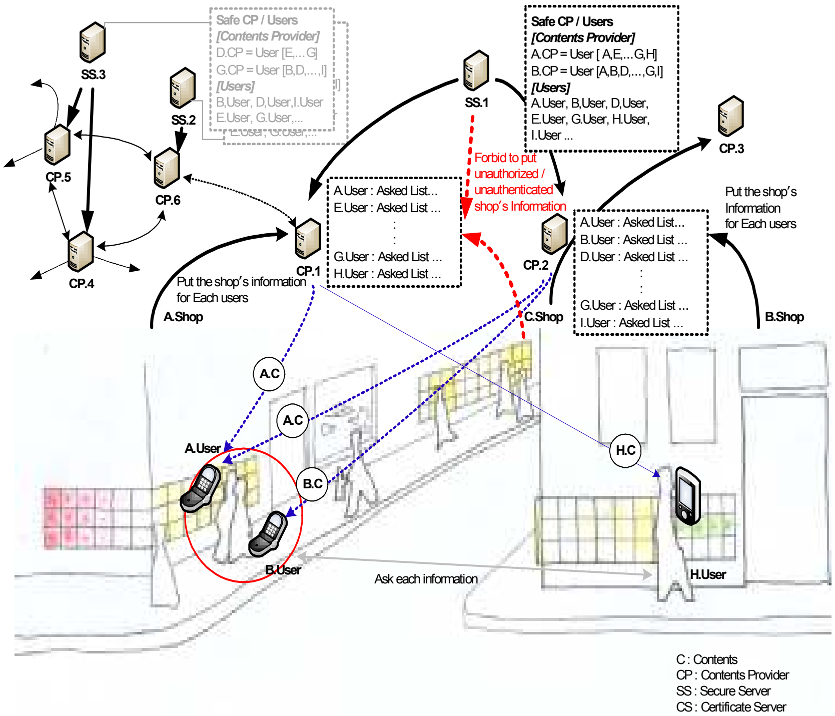

Fig. 2 Urban Life. User A / user B have to register their requesting information before moving.

3.3 Each Step

Each user puts their inquiry into shop computer as shown below. (The shops register them, which the information are related into the CP with shops. CP.1 controls A.Shop and CP.2 manages B.Shop.

// A.Shop.CP.1 / B.Shop.CP.2
A.User's Asking::[/P.1.Cont.2/P.2.Cont.1/]->CP.1
A.User's Asking::[/P.3.Cont.1/]->CP.2
B.User's Asking::[/P.2.Cont.1/P.2.Cont.1/]->CP.2

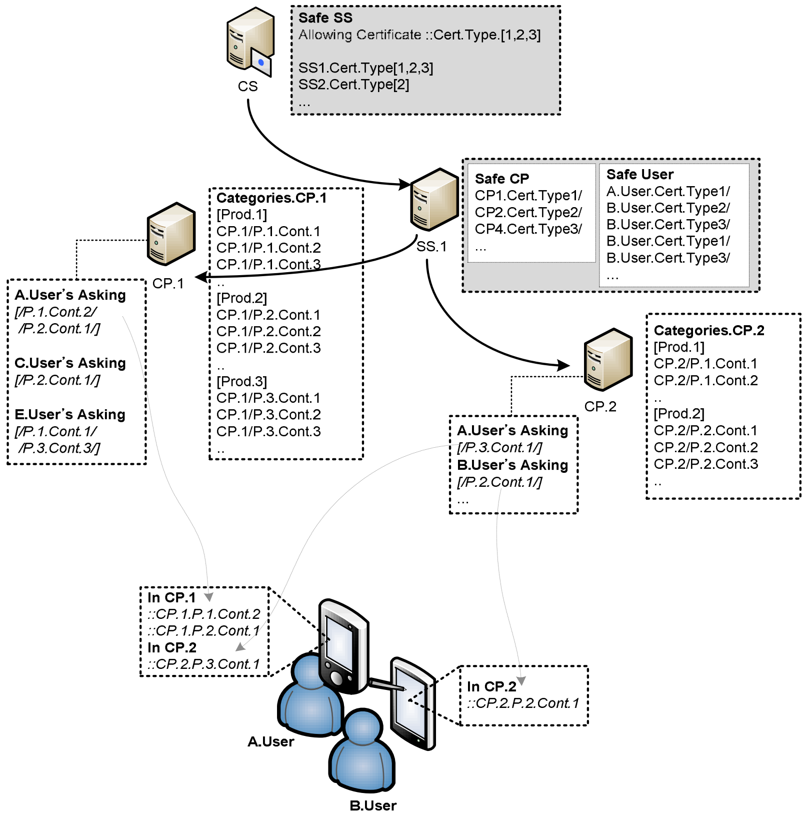

Fig. 3 Each steps

Each CP detects user's movement, when users are in their area. As soon as CP is aware of user.A, it transfers them to user.A.

3.4 Security Processing

If CS gets requesting confirmation of SS from CP, then CS takes and process them. Basically, CS follows the structures and policies of PKI.

SS is responsible for CP and user's authentication. Therefore, SS manages security information for user and CP, it can send the security results to each other if they want it. Also, generally SS processes user's confirmation through CS. With user D, he didn't register his information in CP.1 and SS.1, so CP.1 and SS.1 have no user D's information. Consequently, CP.1 and SS.1 will reject user D without hesitation upon user D's inquiry. [Fig. 4, In red line].

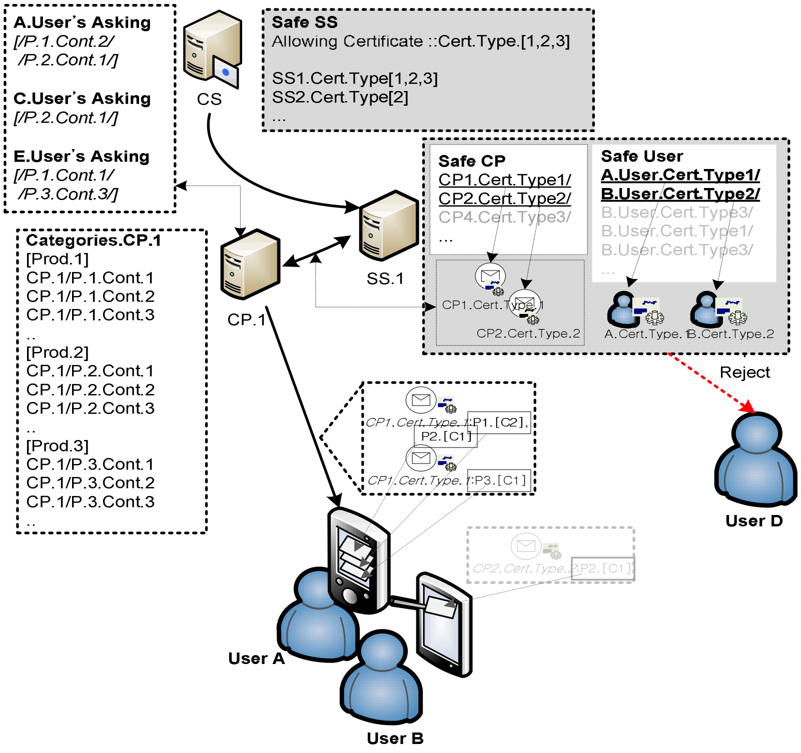

Fig. 4 CP, contents and users certificate. CS keeps security information of SS and SS controls CP and user's.

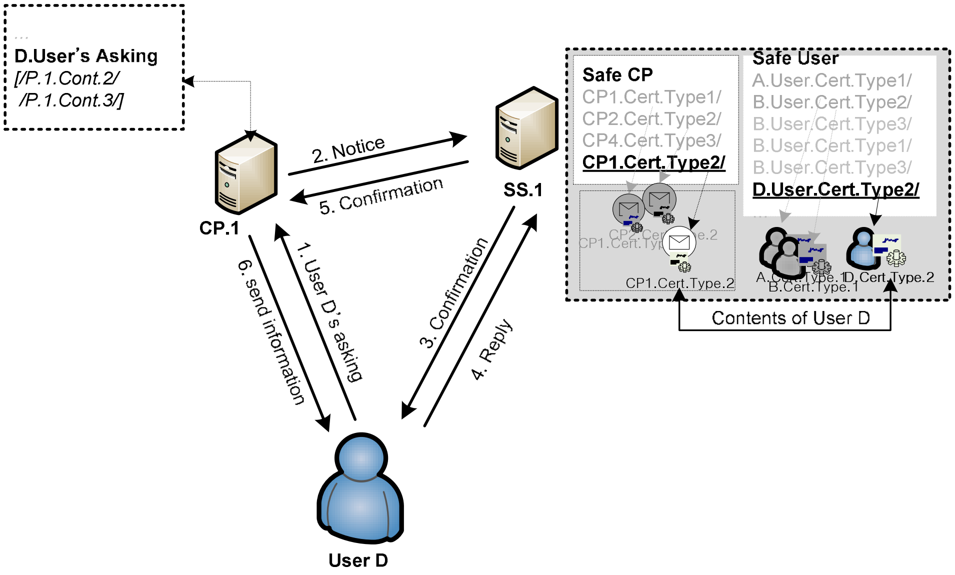

Fig. 5 New user

In the future, if user D wants to receive information of products from the system, first it has to put his request to shop (1). CP.1 transfers user's request information to SS.1, SS.1 take a confirmation for CP.1 / user D (2). Of course, initially SS.1 identifies CP.1 requesting through user D (3)(4). If SS.1 replies the result to CP.1, then all processing will be finished for user D (5)(6) [Fig. 5].

4 Discussion

4.1 Algorithm

The notations in table 2 are used for this article.

Table 2. Notation

Symbol	Contents
x_n	The number of User *(1, 2, ….. , n)*
y_n	Output values of each users =
w_i	Weight (ex, security rate, power, etc)
f_1	Activation function for Users * Weight
f_2	Activation function for Transferring Time * Contents Size
s_n	Contents Size of User *n*
t_n	Transferring Time
T	Critical Values
b	Bios Point
Cost(*C*)	Total Cost

In this research, we suggest that there are *N* users who would be randomly distributed according to the channel of Networks (Shops). Each user moves in their way.

- Model Initial
  - $n = N, T_i = user$ Avg. inactivation time / Arrival schedule of first asking

- Contents asking / processing
  - Processing and contents beginning schedule for arrival
  - $n = n-1$ / $(time() + \exp ntl(T_i / n)) * f(x_n * w_n)$ Next arrival asking schedule

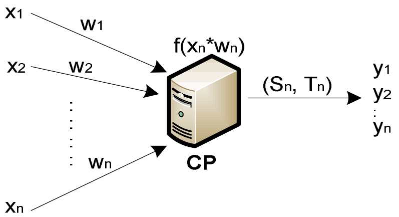

Fig. 6 Cost model

Fig. 6 shows us the cost estimation which happens when the contents are transferred through proposed model. And we put the user's information into proposed algorithm in order to activation point of user, that is, u*sers, weight, message size, transferring time*.

Expression 1 is the cost generation algorithm for *user i*.

$$y_i = f_i(x_i \times w_i) + f_2(s_i \times t_i) \qquad \textbf{(1)}$$

And, we define the algorithm for total cost like expression 2.

$$Cost(C_n) = f_1(x_n \times w_n) + f_2(s_n \times t_n) \qquad \textbf{(2)}$$

Cost for users will be computed with the sum of between (*the number of users* * *weight*, expression 3) and (*transferring time* * *content size*, expression 4).

$$f_1(x_n \times w_n) = x \cdot w^T = [x_1, x_2, \ldots, x_n] \begin{bmatrix} w_1 \\ w_2 \\ : \\ w_n \end{bmatrix} = x_1 \cdot w_1 + x_2 \cdot w_2 + \ldots + x_n \cdot w_n \quad \textbf{(3)}$$

$$f_2(s_n \times t_n) = s \cdot t = [s_1, s_2, \ldots, s_n] \begin{bmatrix} t_1 \\ t_2 \\ : \\ t_n \end{bmatrix} = s_1 \cdot t_1 + s_2 \cdot t_2 + \ldots + s_n \cdot t_n \quad \textbf{(4)}$$

Table 3. Experiment

Items	Contents
The number of CS	1
The number of SS	2
The number of CP	3
The number of CP a user	1.4
The number of User	100
Content Length (Size)	Random (100)
Key Length for Security	512 bits
Link Delay	10ms
Stay Time a User (sec)	Random (100)
Empty CRL Size (Structure)	55kb
Simple Certificate Size	1kb
Experiment Time	1000 sec

Table 3 is the experiment configuration for this paper. The CROSSCERT, which is a security company (VeriSign) in Korea and it is usually assigned with one CRL file per 1000 for certificate. And, there is 55kb size in emptied CRL, each certificate is assigned by 3kb size. However, as a result of the analysis of our certificate, normally, the size of the certificate is to be less and more than 1kb. (Maybe, if we use the expand area of our certificate, that size will be bigger than 1kb in future). Finally, we defined the average certificate size as 1kb in this article.

4.2 Result of Experiments

The number of CP is defined as x_n in experiment. In future, the definition for users will be defined with user's requesting.

CASE 1: User A wants to receive the information from 2 CP, weight of CP.1 is 0.5, CP.2 is 0.3. The content size in CP.1 is 4 and in CP.2 is 2, and then each transferring time is 0.3 and 0.4.

ANSWER 1: $f_1(x_n \times w_n) + f_2(s_n \times t_n)$

$$= \{(2 \times 0.5) + (2 \times 0.3)\} + \{(4 \times 0.3) + (2 \times 0.4)\}$$
$$= 1.6 + 2.0 = 3.6$$

Finally the total cost for user A is 3.6. We applied this algorithm to 100 users with the same way. We let them sequentially enter in experiment area (service area) during experiment time. Table 4 is the result of *average interarrival*, *average waiting time* in queue, average cost.

Table 4. Results

Item	Inter arrival Time	Waiting Time in Queue	Total Cost
Average Time	4.47	3.47	0.57

Average entering time to be in service area is 4.47 sec. The service time from CP after entered that area is 3.47 sec. We called this w*aitingTime* in Queue. This *waitingtime* would be used in Notation 1 as a kind of Weight. Therefore, if *waitingtime* gets longer, *Total Costs* will be increasing. Lastly, *the total cost* for 100 users is 0.57.

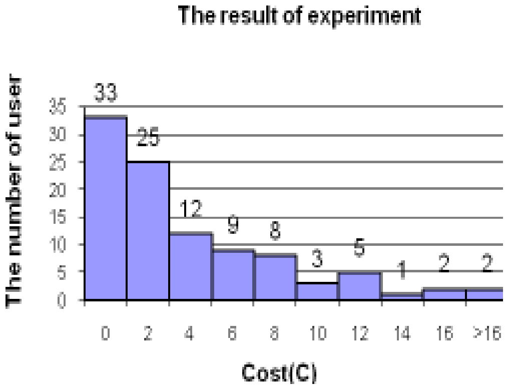

Fig. 7 The result of experiment

Fig. 7 shows us the result of experiment. There are 33 users in between 0 to 2 in total cost that is the minimum cost and the maximum cost is 2 users which cost are 16.

5 Conclusion

We studied the way how users receive their requested information in safety during movement by CP. Of course, we partially put an algorithm for security between users and CPs like authentication. However, still there are some insufficiency points to detailed researching about user's variable, user's and CP's weight etc. Therefore, we need to study those issues in more detail in future, and to have more study a correspondence for security changing of users and CPs.

Acknowledgments

This work is partially supported under the support of the Portuguese Foundation for Science and Technology (FCT) in the aims of Ciência 2007 program for the hiring of Post-PhD researchers.

References

[1.] IST Advisory Group, Scenarios for Ambient Intelligence in 2010, European Commission, 2001.

[2.] Carlos Ramos, Juan Carlos Augusto and Daniel Shapiro, "Ambient intelligence the next step for artificial intelligence," *IEEE Intelligent Systems 2008*, vol. 23, no. 2, Nov. pp. 15-18, 2008.

[3.] Karmen Franinovic and Yon Visell, "Modulating Urban Atmospheres: Opportunity, Flow, and Adaptation," Urban *Computing Conference 2005, Metapolis and Urban Life Workshop Proceeding*, pp. 82-87, 2005.

[4.] Hoon Ko and Carlos Ramos, "A Study on Security Framework for Ambient Intelligent Environment (ISyRAmI SF : ISyRAmI Security Framework)," *ICWMC2009*, pp. 93-98, 2009.

[5.] Mingchao Ma, "Authorization delegation for u-City in subscription-based," *Computers & Security*, pp. 371-378, 2006.

[6.] Stephen J. H. Yang, "Context-Aware Ubiquitous Learning Environments for Peer-to-Peer Collaborative Learning," *Educational Technology & Society, Security*, pp. 188-201, 2006.

[7.] Chen, G., Kotz, D, A Survey of Context-Aware Mobile Computing Research, Technical Report: TR2000-381 Dartmouth College: Hanover, NH, USA.

[8.] Ward, A., Jones, A., & Hopper, A, "A new location technique for the active office," *IEEE Personal Communications*, vol. 4, no. 5, pp. 42-47, 1997.

[9.] Mingchao Ma, "Authorization delegation for u-City in subscription-based," *Computers & Security*, pp. 371-378, 2006.

[10.] Rene Meiier and Vinny Cahill, "Location-Aware Event-Based Middleware: A Paradigm for Collaborative Mobile Application," *Computers & Security*, pp. 371-378, 2006.

[11.] Stephen J. H. Yang, "Context-Aware Ubiquitous Learning Environments for Peer-to-Peer Collaborative Learning," *Educational Technology & Society, Security*, pp. 188-201, 2006.

[12.] Mardoqueu Souza Vieira and Nelson Souto Rosa, "A Reconfigurable Group Management Middleware Service for Wireless Sensor Networks," *MPAC 2005*, pp. 1-8, Nov. 2005.

[13.] Thirunavukkarasu Sivaharan, Gordon Blair and Geoff Conlson, "GREEN: A Configurable and Re-configurable Publish-Subscribe Middleware for Pervasive Computing," *CoopIS/DOA/ODBASE2005 (LNCS) 3760*, pp. 732-749, 2005.

[14.] Hua Si, Yoshihiro Kawahara, Hisashi Kurasawa, Hiroyuki Morikawa and Tomonory Aoyama, "A Context-aware Collaborative Filtering Algorithm for Real World Oriented Content Delivery Service," Ubiquitous Computing Conference,Metapolis and Urban Life Workshop Proceedings, September, pp. 65-68, 2005.

[15.] Stephen J. H. Yang, "Context-Aware Ubiquitous Learning Environments for Peer-to-Peer Collaborative Learning," Educational Technology & Society, Security, pp. 188-201, 2006.

[16.] Mardoqueu Souza Vieira and Nelson Souto Rosa, "A Reconfigurable Group Management Middleware Service for Wireless Sensor Networks," MPAC 2005, November, pp. 1-8, 2005.