Extending the UbiMDR Supporting Situation-Aware Access Control

Jeong-Dong Kim[1], Dongwon Jeong[2*], and Doo-Kwon Baik[1*]
[1]*Dept. of Computer Science & Engineering, Korea University,*
[2]*Dept. of Information Sciences, Kunsan National University*
kjd4u@korea.ac.kr, djeong@kunsan.ac.kr, baikdk@korea.ac.kr

Abstract

Ubiquitous computing environment requirement needs information sharing of sensors based on sensor network technology, situation-aware and determination functions and other related technologies ranging to appropriate and effective action processing. The sensor field independent information access is most important issues in everywhere under the ubiquitous computing environment. We already proposed UbiMDR framework that is a supporting Application-Independent Semantic Interoperability for Ubiquitous Applications. However, the functions of the UbiMDR are limited only to identification and recognition of objects. The chief objective of our proposal is to let extending the UbiMDR supporting situation-aware access control about objects consistently and independently on various application fields (companies/ systems). This paper fist describes the current UbiMDR, and presents our proposed model for supporting situation-aware of UbiMDR. Also conceptual architectures of situation aware are shown.

Keywords: *UbiMDR, Situation-aware, access control.*

1. Introduction

Ubiquitous computing [1-3] encompasses a wide range of research topics, including distributed computing, mobile computing, sensor networks, human-computer interaction, and artificial intelligence. Ubiquitous computing has also a variety of terms in use to describe Pervasive Computing and Ambient Intelligence. The goal of ubiquitous computing environments is to integrate the pervasive systems so as to optimize them with their surrounding circumstances, and provide user-customized service.

There are many issues such as energy management, protocol standardization, supporting the situation-awareness, independency on sensor fields, and security to be resolved for the complete ubiquitous computing.

Especially, the sensor field-independent information access is one of the most important issues to maximize the usability of sensors in various sensor fields [4], [5]. To solve this problem (independency on sensor fields), we already proposed the UbiMDR that is a MDR-based framework to provide sensor field with independent semantic interoperability in ubiquitous computing environment [6]. But, the ubiquitous computing environment will require a variety of applications and utilizations of the UbiMDR. In other word, the function of the current UbiMDR are limited only to identification and recognition of objects. The most promising one of the existing research issues related to ubiquitous computing is situation-awareness. Accordingly, the UbiMDR will be extended to support the situation-awareness

This paper is supported by the Brain Korea 21 Project.
*Corresponding authors

concept. In this paper we will define situation and present a method to develop situation-aware application capable of analyzing both contexts and user actions.

The rest of this paper is organized as follows. Section 2 describes related work. Section 3 presents our proposed approach model, the definition of use policy, conceptual architecture in this paper. Section 4 concludes this paper.

2. Related Work

This section describes a situation-aware technology for UbiMDR supporting the situation-awareness access control. As well as, we explain the UbiMDR conceptual model, and also present the uMDR its structure.

2.1. Situation-Aware Technology

Recently, ubiquitous computing, which is considered as a new computing paradigm, is accessible to networks anywhere and anytime. For such an environment, characteristics such as situation-awareness, context-sensitivity, Ad-hoc communication should be provided.

- **Situation-awareness:** Situation awareness is the capability of a device to capture and analyze the relationship among multiple contexts and actions over a period of time.
- **Context-sensitivity:** Context sensitivity is the capability of a device to detect its current context and changes in contextual data.
- **Ad-hoc communication:** Communication channels among application tend to be instantaneously established and terminated due to changing contexts, device mobility, and resource availability.

Situation-awareness analyzes and examines relationship between actions and multiple contexts in view of time changes. In other words, situation-awareness means that devices are able to take actions automatically and timely depending on situations. These successive processes are performed depending on situations, not at a certain time interval. Not that the actions are processed depending on time, place, or the user behavior, but that the actions are processed through the situation-awareness and inference.

The sensor of UbiMDR framework needs language and architecture for providing the situation-awareness technology and enhancing its utility.

2.2 uMDR

The MDR has been developed to maximize the semantic interoperability between databases world by ISO/IEC JTC 1/SC 32 [7]. The MDR has been used to implement applications in various domains [8-10] and develop frameworks to facilitate sharing and exchanging of data. We employ the advantages of the MDR to achieve the semantic consistency of data in ubiquitous environment.

However, the original MDR is more complicated for the ubiquitous applications, thus the definition of an optimized MDR is need to be suitable for the ubiquitous environment. It means ubiquitous application the data set from sensors is smaller than the data set used in database (application) level.

Figure 1 shows the uMDR metamodel for the UbiMDR. Compared with the original MDR, a novelty of the uMDR is the integration of the Data_Element_Concept and Conceptual_Domain, which result in a Conceptual_Identifier.

The benefit brought by this integration enable the management of data element concept with a less storage cost. The uMDR attributes of each component are illustrated as the figure 2.

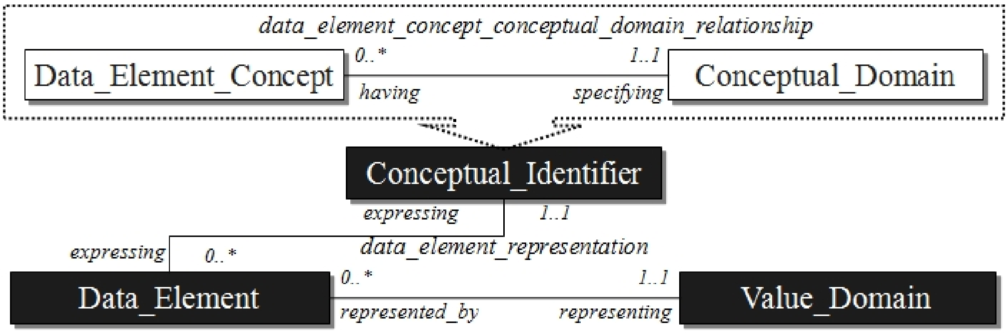

Figure 1. Concept model for the uMDR.

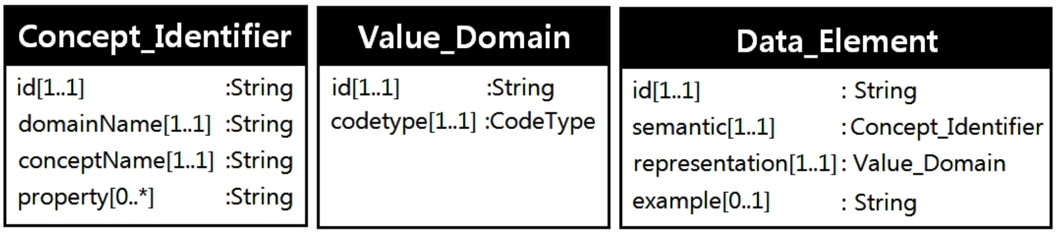

Figure 2. Attributes of uMDR components.

2.3 UbiMDR

Figure 3-B shows the conceptual model for the UbiMDR. In the figure 3, Sensors (RFID tags) straggle at the every sensor fields that might move or not in ubiquitous environment. The uMDR contains predefined values (data element) for semantic interoperability, and because of this, these uMDR can be useful in reducing the cost by for the most effectively used of supporting semantic interoperability in variety sensor fields. In other words, information of sensors as well devices is formed according to the uMDR. In this conceptual model of UbiMDR are used for the semantic interoperability between sensors and devices/applications [6].

3. Proposed Model

In this section describes the situation-awareness and representation method of use policy, and also present conceptual architectures of SA-UbiMDR.

3.1. Use Policy of SA-UbiMDR

The SA-UbiMDR, which is suitable for the ubiquitous computing environment, enhances usability of the sensor system (RFID system) by use of information acquired from various sensors. The proposed SA-UbiMDR is capable of recognizing such a situation and determining the use of the resource based on the recognized situation information. We suggest architectures for the SA-UbiMDR capable of recognizing the situation and taking suitable actions. The SA-UbiMDR for the ubiquitous computing environment requires the development of sensor network technology and network technology for high-rate communication and integration of situation-awareness technology. Now that the ubiquitous computing environment requires various use policies for the existing sensor system, simple reading operation of the current sensor (RFID tag) information is insufficient to satisfy that requirement.

Appropriate operations need to be allowable using situation information from adjacent sensors and information from the sensor. The implementation of the situation-based use policy requires the following technologies.

- **Use policy definition and representation method:** How to define and represent the use policy depending on situation.

To address the requirement, we propose Situation Awareness-Identification Language (SA-IDL) on the basis of five W's and one H (5W/1H), basically used by human for situation determination.

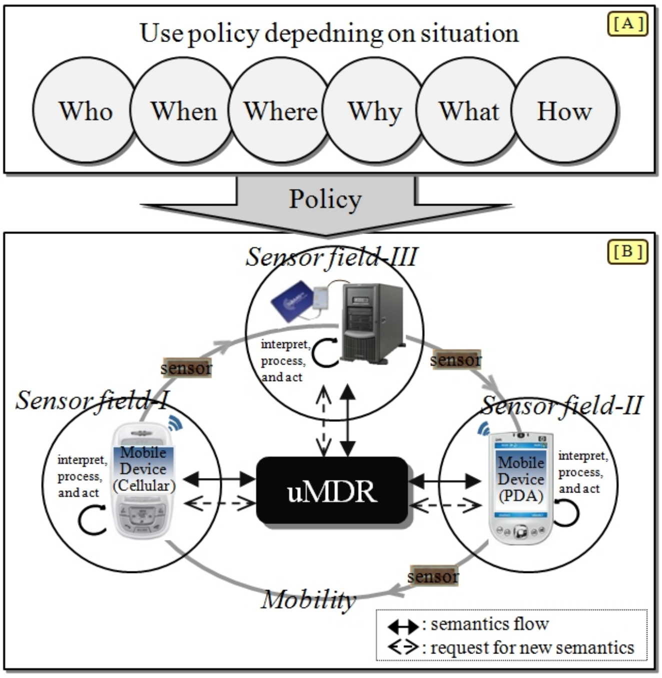

Figure 3. Concept of SA-IDL.

Figure 3-B depicts concepts of the SA-IDL. The SA-IDL is classified into a user (WHO) policy, an access location (WHERE) and access time (WHEN) policy, an access purpose (WHY) policy, an accessible valid information (WHAT) policy and an access method (HOW) policy, the SA-IDL has been modified fit for the SA-UbiMDR in the ubiquitous computing environment, so at to handle complexity of SA-IDL proposed in [11].

```
SA-IDL
who:PowerSet WHO={who1, who2, …}
wher: PowerSet WHEN={before, after, now, 10:31, ..}
where: PowerSet WHERE={lab, seoul, {(10, 10),
                                   (100, 400)}, …}
why: PowerSet WHY={why1, why2, …}
what: PowerSet WHAT={what1, what2, …}
how: PowerSet HOW={read_only, write, store, …}
-----------------------------------------------
Who ≠ { },
What ≠ { }
```

```
situation Retailer {
definition:
      who: Retailer
task:
      who: Supply Chain Management;
      what: producing_district_information;
      when: now;
      doing: read;
   }
```

Figure 4. Basic Structure of SA-IDL. Figure 5. Use policy *WHO* of SA-IDL.

Figure 4 systematically represents general concept of the SA-IDL based on 5W/1H by a formal language Z. In figure 4, the SA-IDL includes six attributes for the representation of the use policies in the SA-UbiMDR. Each attribute may consist of mandatory attributes or optional attributes according to applications. WHO and WHAT policies, that is, who and what attributes are defined as mandatory attributes. Accordingly, who and what attributes have to contain more than one element excluding an empty set. Characteristics of the attributes may be defined variously depending on environment and applications.

Let's assume that we want to access of product information to be blocked by users of a previous process after a certain process in Supply Chain Management (SCM) [12]. Provided that a subject of the current access is a 'Retailer' is limited to original information, use policy *WHO* of SA-IDL is represented as show figure 5

The defined SA-IDL is divided into a definition and task part. The definition part defined a subject being monitored for the SA and the task part describes permitted authorization scope and actions. The above definition language means that the subject is a retailer and the target object is SCM. Also the definition shows the retailer can access (read) information of SCM.

Alternatively, privacy protection policy depending on sensor (RFID tag) information may be defined as the use policy protection policy as follows: Improper access, improper collection, improper monitoring, improper analysis, improper transfer, unwanted solicitation, improper storage. By accepting the above invasion types, how to use personal information relating to the sensor is represented in HOW and its access methods and defined as below:

- Access to personal information resource.
- Collection of the personal information resource, or, collection of personal information using the personal information resource.
- Monitoring on the personal information resource, or, monitoring using the personal information resource.
- Analysis on the personal information resource, or, analysis using the personal information resource.
- Transferring of the personal information resource, or, transferring of the personal information resource.
- Storing of the personal information resource.
- Solicitation of service object.

There access methods are represented in the SA-IDL as below:

```
situation Retailer {
definition:
        who: Retailer
task:
        who: consumer;
        what: producing_information;
        when: always;
        doing: only access;
        }
```

Figure 6. Access methods in SA-IDL.

The retailer can only access (read) to information on items purchased by the consumer and cannot monitor, collect, delivery, transfer, or store the information. As shown in the above example, the usability of the SA-UbiMDR is elevated because of assigning various use policies of the sensor.

3.2 Conceptual Architectures of SA-UbiMDR

We describe a management method of the situation-based use policy for sake of valid access management on sensor (RFID tag) information of the SA-UbiMDR.

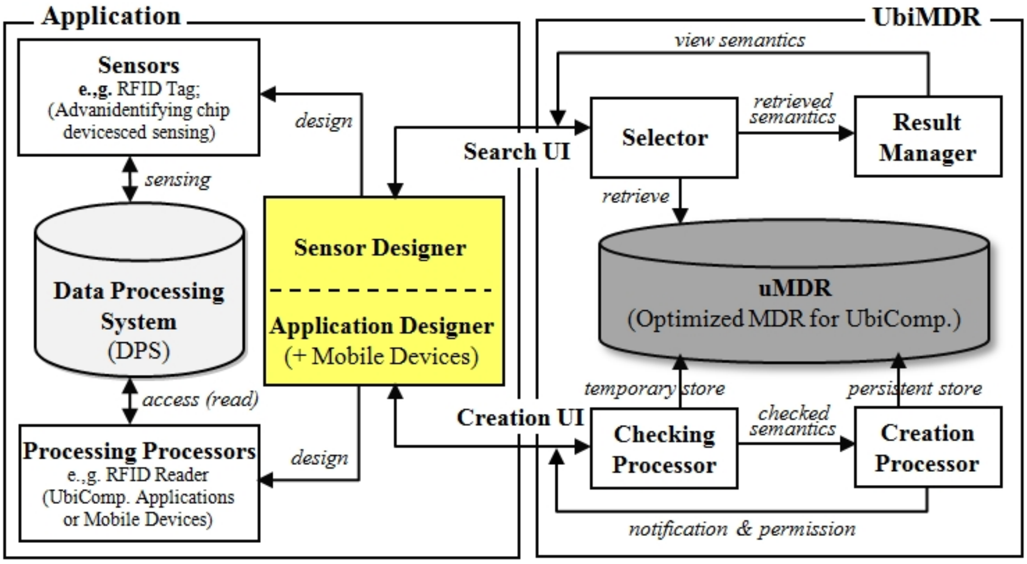

Figure 7. Architecture concept of SA-UbiMDR.

In figure 7, the Sensors (RFID Tags) holds ID information of an object and it is the same as the traditional current sensors function. The Processing Processors (RFID reader) reads information from the sensors. In addition, in case of the SA-UbiMDR architecture, the Processing Processors can provides extended functions that can acquire situation information from sensors, infer proper actions from the situation information and execute the actions.

The Data Processing System (DPS) basically utilizes the information acquired by the RFID Reader. The DPS also contains information pertaining to the use policies and determines suitable actions by inferring and judging the situation information.

For supporting the situation-awareness technology, the sensor system requires functions to collect situation information define use policies with a profitable representation language and infer for determining valid action using the use policies and the situation information collected. We satisfy these requirements by applying the concept of the situation-awareness. The types of the SA-UbiMDR architecture in the study are selected depending on which components collect and infer the situation information.

4. Conclusion

The ubiquitous computing is considered as the next generation computing paradigm. Many sensors will be able to provide various and abundant situation information in the ubiquitous computing environment. In this paper, we described the extending the UbiMDR supporting situation-awareness access control. We proposed the use policies and a formal language for the expression of the use policies to support the situation awareness concept in the ubiquitous computing environments, suggested of SA-UbiMDR architecture.

In the future, the extension and refinement of specification language for SA-UbiMDR are needed. Additionally, the study for inference engine is needed in order to provide a quick and accurate response.

References

[1] Weiser, M.: http://www.ubiq.com/hypertext/weiser/Ubi- Home.html.

[2] Jeong, D., Kim, Y., In, H, "New RFID System Architectures Supporting Situation-Awareness under Ubiquitous Environments," Journal of Computer Science, Vol. 1, No. 2, Science Publications, pp.114-120, Aug.2005.

[3] Yau, S, S, and F. Karim, "Adaptive middleware for ubiquitous computing environments", Proc. IFIP WCC, August, 2002.

[4] IIyas, M., Mahgoub, I., "Handbood of Sensor Networks: Compact Wireless and Wired Sensing Systems," CRC Press, Jul 2004.

[5] D. Jeong, L-S. Lee, "A New MDR-based RFID System Architecture for Ubiquitous Computing Environment," Journal of Korea Society for Simulation, vol.14, no.4, pp.43-53, Dec 2005.

[6] J. Kim, D. Jeong, Y. Jing, D-K. Baik, "UbiMDR: Supporting Application-Independent Semantic Interoperability for Ubiquitous Applications," Computational Intelligence and Security, pp. 1155-1158, Nov.2006.

[7] ISO/IEC JTC 1/SC 32, ISO/IEC 11179: Information Technology-Metadata Registries - Part 1 ~ Part 6, 2004.

[8] Environmental Protection Agency (EPA), Environmental Data Registry (EDR), http://www.epa.gov/edr/

[9] Australian Institute of Health and Welfare, Australian National Health Information Knowledgebase, http://www.aihw.gov.au/ (2008).

[10] U.S. Department of Transportation, U.S. Intelligent Transportation System (ITS), http://www.dot.gov/ (2008).

[11] Yau, S., Y. Wang and and F. Karim, "Developing situation-awareness in middleware for ubicomp environments", Proc. International computer software and applications conference, pp.233-238, 2002.

[12] Daugherty, P.J., T.P.Stank and D.S.Rogers, "Third-party logistics service providers: Purchasers perceptions", The J. Supply Chain Management, pp.23-29, 1996.

Authors

Jeong-Dong Kim He received the MS degree in Computer Science from Korea University in 2008. He is a Ph. d student in the department of computer science and engineering, Korea University, Seoul, Korea since 2008. His research interests include Metadata-based integration, Semantic Web, Data Engineering, and Access Control in the Ubiquitous Computing.

Dongwon Jeong He received his BS degree from Kunsan National Univ. (1997), his MS degree from Chungbuk National Univ. (1999), and his Ph.D. degree from Korea Univ. (2004), all in computer science and all in Korea. He was a Research Assistant Professor in the Research Institute of Information & Communication Technology, Korea Univ. (2004~2005). He was a Visiting Research Scholar (Post-Doc.), School of Information Sciences & Technology, Pennsylvania State University, USA. He is a Committee Member of the Telecommunication Technology Association, Korea (2002~present) and a Korean National Committee Member, ISO/IEC JTC 1/SC 32, Korea (2006~present). He is an Assistant Professor in the Department of Informatics and Statistics, Kunsan National University, Korea. His research interests include metadata-based integration, mobile agent security, ubiquitous computing & semantic maintenance, and ontology conversion.

Doo-Kwon Baik received his B.S. degree in Mathematics from Korea University, Seoul, Korea, in 1974. He received his M.S. and Ph.D. degrees in Computer Science from Wayne State University at U.S.A., in 1983 and 1986, respectively. He is a full professor in the department of computer science and engineering, Korea University, Seoul, Korea. Also, he is a committee chair of ISO/IEC JTC1/SC32- Korea. His research interests include data engineering, software engineering, and modeling and simulation.