Journal of Korea Multimedia Society Vol. 15, No. 12, December 2012(pp. 1475-1484)

Context-based Authentication Service for The Mobile Office

Jiyoung Yang[†], Hyundong Lee[††], Shi-Kook Rhyoo[†††], Mokdong Chung[††††]

ABSTRACT

Today many companies introduce new mobile office environments evolved from the recent rapid development in mobile device technologies. Most of the recent mobile office systems use a simple authentication scheme such as ID/Password. This method is easy to use, but it does not consider the user's context. Thus it cannot provide appropriate security service required by the user's proper contexts. Therefore, this paper proposes a context based authentication system which applies security level verification and uses fuzzy algorithm based on the importance of access authority control.

Key words: Context-Awareness, Mobile Office, Fuzzy Theory

1. INTRODUCTION

Most of the recent mobile office systems use a simple authentication technique which is based on ID/Password. This method has the possibility of leakage of personal information and the company's confidential information since the mobile devices can be stolen or lost. And there can be possible security threats when we access an illegal intranet server via the smartphone. Recently, security threats against mobile devices have been increasing because users store personal data in their mobile devices which are exposed to the mobile networks that are vulnerable to cyber attacks[1].

To deal with these security threats, the mobile device needs to employ security functions such as firewall, IDS, and virus scanner. However, when these functions are applied on the mobile device, various problems arise such as performance deterioration and/or inconvenience owing to poor computing power, lack of computing resource or convenient user interface[2]. One example of convenience is that users tend to use a simple and tiny password such as 0000, 1234 for their convenience. This means that the probable exposure of ID/Password might be increased.

We developed a context-based authentication system to cope with these problems. Mobile office's context-based authentication system goes through the identity verification process by analyzing the user's access pattern when he or she logs in to the system. After the basic authentication process is finished with ID/Password, it collects the user's context information (time, location, USIM(Universal Subscribe Identity Module), and cell phone number) and quantifies the access pattern value. And it compares and analyzes the process by using this quantified value. Whenever it

※ Corresponding Author : Mokdong Chung, Address : (608-737) Dept of Computer Engineering, 599-1, Daeyeon 3-Dong, Nam-Gu Busan Korea, TEL : +82-51-629-6253, FAX : +82-51- 629-6264, E-mail : mdchung@pknu.ac.kr
Receipt date : Sep. 24, 2012, Revision date : Nov. 10, 2012
Approval date : Nov. 27, 2012
† Dept. of Computer Engineering, Pukyong National University, Korea
(E-mail: na090@hanmail.net)
†† Dept. of Computer Engineering, Pukyong National University, Korea
(E-mail: win4class@hanmail.net)
††† Division of Info. Tech., Kyungnam College of Information & Technology, Korea
(E-mail: skrh99@kit.ac.kr)
†††† Dept. of Computer Engineering, Pukyong National University, Korea
※ This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2010-0024053).

classifies the validity of identifying personal information as low, the system requires additional authentication. Our authentication system's validity of identifying personal evaluation makes some ambiguous results hard to convert to numeric values such as 'very accurate', 'accurate', or 'normal'. Thus the system has problems in making precise decisions regarding the system's validity.

Therefore, to solve this problem, we adopted the fuzzy algorithm which deals with ambiguous problems and proposed a method of enhancing the validity of this context-based authentication system. This method improves on the existing method in which the administrator adjusts security configurations by manually operating and modifying the system for the optimal security configurations. Thus our mechanism improves the system's efficiency, security, and convenience.

The structure of this paper is as follows: Section2 describes the works related to context awareness, AHP, and fuzzy algorithm. Section 3 deals with the context based authentication system. Section 4 explains the validation and optimization of the proposed security system. Finally, Section 5 presents the results of the paper and shows possible directions for further research.

2. RELATED WORK

2.1 Context Awareness

The first definition of context-aware technology given by Schilit[3] is that 'context-aware software adapts according to the location of user, the collection of nearby people, hosts, and accessible devices, as well as to changes to such things over time.'[4].

Most research on context information processing (CoBra[5], Gaia[6], SOCAM[7], CAMUS[8], [9]) is related to collecting information and providing service, but it is difficult to verify whether the inference is appropriate or not. The proposed system in this paper has been structured to flexibly select the context information and function in order to give relevant appropriate feedback during the operation of the context aware security service, thereby providing more appropriate security service.

2.2 AHP (Analytic Hierarchic Process)

AHP is a decision problem that consists of a number of evaluation elements for the evaluation component layering in accordance with the hierarchy of importance (weight), but in the decision making process, it is not easy for users to choose appropriate attribute by considering a variety of number of cases[10].

The analytical hierarchical process (AHP) not only adopts a qualitative method of reducing an unstructured problem into a systematic decision hierarchy but also uses pairwise comparison to perform the consistency examination[11].

2.3 Fuzzy algorithms

In 1965, Zadeh[12] proposed the fuzzy set theory, which is based on the ambiguity contained a mathematical model of uncertainty. Especially, when we deal with human's subjective recognition which cannot handle probability matters, it is useful for risk analysis of the uncertain atoms which have no certain boundary between the atoms in the collective group and those that are not in the collective group. In general, when element x belongs to crisp set A, the membership function $\mu_A(x)=0$ and, therefore, the value of the membership function becomes 1 or 0. In other words, the membership function μ_A in the crisp set maps all the elements only as {0, 1} in the universal set X. In contrast, the fuzzy set enables the membership function to have not only 1 and 0 but also have an arbitrary real number between 1 and 0. The possibility of element x to belong to fuzzy set A is expressed as $\mu_A(x)$ and the value of this possibility is the real number between 1 and 0[13].

Our authentication system's validity of identify-

ing personal evaluation makes some ambiguous results hard to convert to numeric values such as 'very accurate', 'accurate', or 'normal'. Therefore, we applied the fuzzy algorithm in choosing evaluation elements such as user's estimation grade, intrusion detection, and risk of intrusion.

We propose a method of evaluating the system validity by using the following three categories of information as shown in Fig. 1.

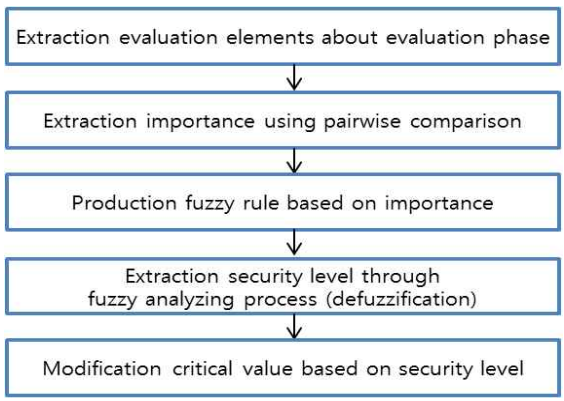


Fig. 1. System Validity Evaluation Flowchart.

3. CONTEXT BASED AUTHENTICATION SYSTEM

3.1 Overview of the System

To deal with security threats, the mobile device needs to employ security functions such as firewall, IDS, and virus scanner. However, when these functions are applied on the mobile device, various problems arise such as performance deterioration and/or inconvenience because of poor computing power, lack of computing resource and inconvenient user interface.

This paper presents an additional authentication which uses personal and context information contextually in addition to ID/password authentication.

This method analyzes the accuracy of identity verification by comparing the user's current access pattern with individual average access pattern and by determining whether additional authentication is necessary. Fig. 2 shows the overview of the proposed context based authentication system.

- Smart Phone: When a user logs in to mobile office, the system collects the context information and performs identity verification. The user authentication information and the context information are passed from the Security Agent in the Security Server to the Context Manager. We use a block cipher, SEED, for data confidentiality in socket communication.
- Security Server: The security server analyzes the context information. The access type is quantified and compared with the value of Login Pattern DB to determine whether additional authentication is necessary.

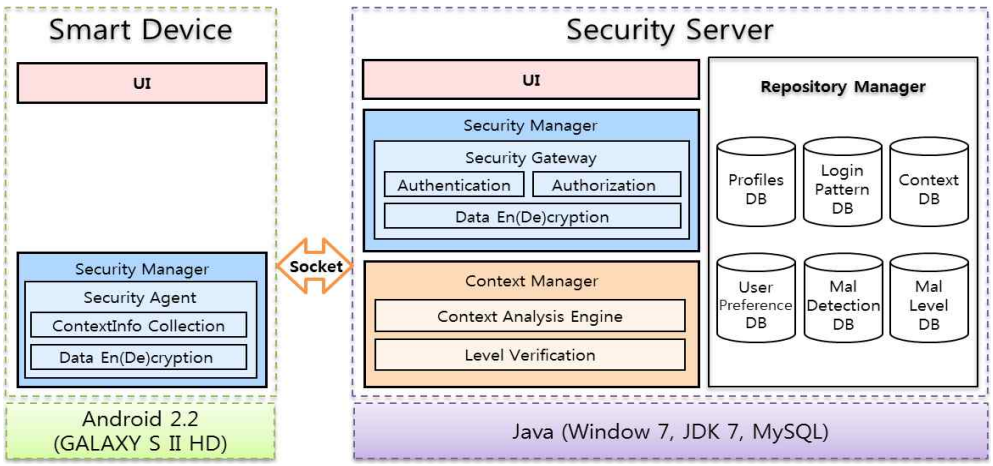


Fig. 2. Overview of the Proposed System.

3.2 Process of Determining whether Additional Authentication

The new context based authentication system collects the user's context information (time, location, USIM and phone number) for the analysis and quantification after the basic (ID/password) authentication. First, time information is determined by the user's log in time, and access location is determined by the network. If someone accesses the network by using WIFI(wireless fidelity) communication in a company, we figure out the user's location that is in the company, and if people use 3G, we determine that the location is outside the office. USIM information uses IMEI(International Mobile Equipment Identity) of USIM card. Finally the user's access pattern is quantified and analyzed by using the context information(location, time, USIM and phone number). This method analyzes the accuracy of identity verification and determines whether additional authentication is necessary or not by using the quantified value.

This context information is transmitted to Security Server of the proposed system as shown in Fig. 2. First, the proposed system collects context information from the mobile devices and provides proper weight value with corresponding weight factor according to its current context. These weight values may be changed due to their feedbacks. If the calculated level is low, our system classifies the security state as unstable and enhances security strength. On the other hand, if calculated level is high, the system classifies security state as suitable and provides normal mobile office services.

Through this process, the proposed system calculates the new average level by comparing the user's average level with the user's current access pattern.

Fig. 3 shows a comparison of individual average access pattern level and current access pattern level. The proposed system checks whether the deviation is greater than the standard. If the difference between the current access level and the average access level is greater than the security level(critical value, Θ), the validity of the user's identity is classified as low and then additional authentication is requested. The security level (critical value, Θ) is the decisive value for the determination of additional authentication. The new context based authentication system defines the

Table 1. Level of Location

	work	home	outside the work	overseas
Location	1(standard)	standard*0.5	standard*0.3	standard*0.1

Table 2. Level of Time

	business hours	business hours±2	business hours more than±2
Time	1(standard)	standard*0.3	standard*0.1

Table 3. Level of USIM

	own USIM	other USIM
USIM	1(standard)	standard*0.1

Table 4. Level of Phone number

	own phone number	other phone number
phone number	1(standard)	standard*0.1

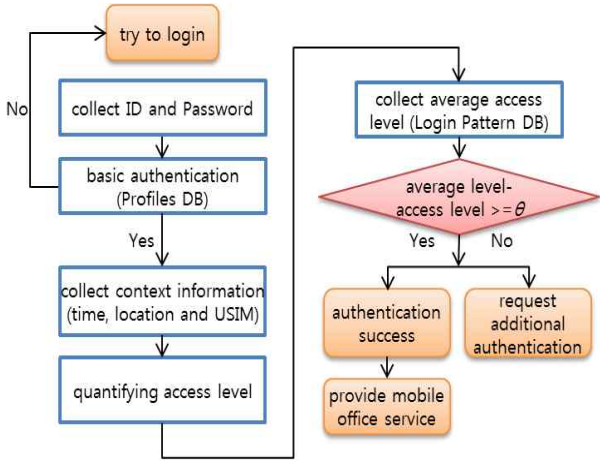


Fig. 3. Process of Additional Authentication.

default value of 0.5 as the security level (critical value, Θ) and adjusts it automatically in accordance with the security level. The proposed system calculates the user's access pattern by using the current access pattern and the existing access pattern in databases. Through this process, the administrator can control user's access type automatically.

4. VALIDATION AND OPTIMIZATION OF THE PROPOSED SECURITY SYSTEM

The new context based authentication system modifies the security level(critical value, Θ) based on context information. The only measure for verifying and modifying the security level is the user's response at the real field and it is hard to make an accurate analysis. To solve this problem, we deducted three evaluation factors for investigating the system's validity based on the feedback from the manager and the hands-on workers.

We define the three elements for optimization of the security level as follows.

① Evaluation grade: The evaluation grade represents the degree of user's satisfaction. The higher evaluation grade means the greater stability and efficiency of the system.

② Intrusion detection: If the system detects many intrusions, it classifies the system as unstable.

③ Risk of intrusion: If an intrusion is detected, the risk of intrusion is measured on the basis of the data stored in the database. Risk of intrusion is classified as low, medium and high based on the information security standard offered by CVE[14].

4.1 Fuzzy Rule Configuration

We can collect data from books, computer databases, flow charts, behavioral observations, surveys, brainstorming, etc, to compose fuzzy rules [15]. Each evaluation factor for verifying the security level has different weighted value depending on evaluators, so we calculate each evaluation factor's importance by using AHP. The AHP procedure is applied as follows. First, we set evaluation elements and structuralize the elements. Second, we calculate the importance among the elements and determine their priority.

In this paper, we use a methodology proposed by Chang[16] in 1996 to calculate the importance. First, we define evaluation factors as shown in Table 5. Then, our new context based authentication system performs pairwise comparison in estimation of the same level as in Table 6 and calculates the importance from the matrix. Assuming that matrix A is as follows,

$$A=\begin{bmatrix} 1 & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & 1 & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & 1 & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & 1 & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & 1 \end{bmatrix}$$

if $i=j$, satisfy any $a_{ij=\{1,1,1\}}$ and

Table 5. Process of Importance Calculation

a_{ij}	Description
1	Equal Importance
2	Moderate Importance
3	Extreme Importance
Inverse number	Reciprocal of the importance that correspond to the inverse importance

Table 6. Process of Importance Calculation

	high grade	low grade	many detection	few detection	high risk	low risk
high grade	1	1/3	1/3	1/2	1/3	1/2
low grade	3	1	1/2	3	1/2	3
many detection	3	2	1	3	1	3
few detection	2	1/3	1/3	1	1/2	1
high risk	3	2	1	2	1	3
low risk	2	1/3	1/3	1	1/3	1
⇩						
	high grade	low grade	many detection	few detection	high risk	low risk
importance	0.067	0.201	0.275	0.102	0.260	0.094

$l_{ij}=\frac{1}{l_{ji}}$, $m_{ij}=\frac{1}{m_{ji}}$, $u_{ij}=\frac{1}{u_{ji}}$ is established.

The importance among the six evaluation factors is high when there are many cases of intrusion detection, high risk of detention, low evaluation grade from users. We make 27 fuzzy rules reflecting the conducted importance. This method of multiplying weights can be controlled by the administrator with a heuristic method depending on the work type. If the user's real access and proposed additional authentication are not good, we can change the weighted value.

4.2 Fuzzy Inference Process

The proposed context based authentication system is capable of protecting the confidential information through appropriate identity verification and also of modifying the security level automatically whereas the existing system is operated manually for modification security level. However, it is not easy for users to choose appropriate attribute by considering a number of various cases. Therefore, we use a fuzzy algorithm for resolving this problem. We use evaluation grade, intrusion detection and risk of intrusion information for input values.

Fig. 4 shows the process of defuzzification. The range of the membership function is [0, 1], and the defuzzification value is estimated to be 0.718 when the membership function is 1, 0.1, 0, respectively.

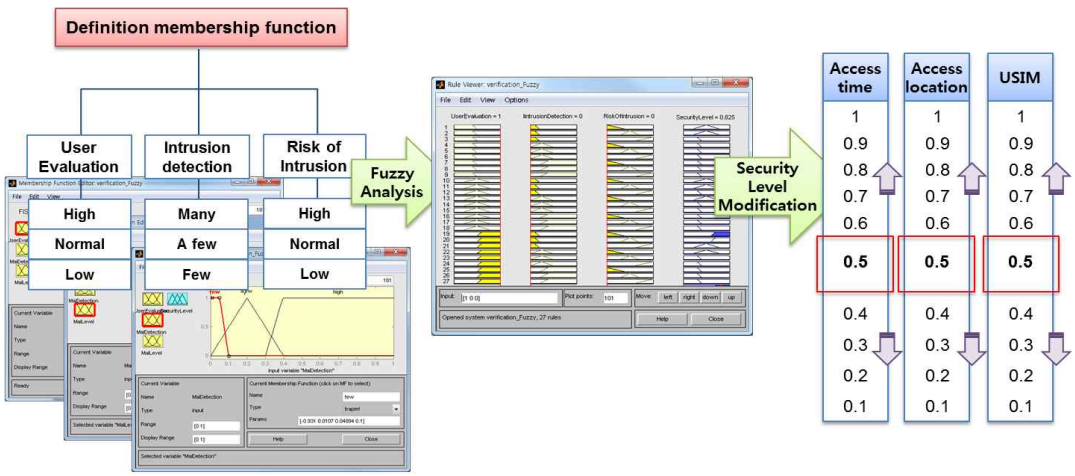


Fig. 4. Process of Fuzzy Analysis.

Convenience is offered to the user by automatically changing the security level on the basis of the estimated value, and the risk of the defuzzification value is overcome.

4.3 Evaluation of the Proposed Security System

To verify the convenience, security and efficiency, we performed system evaluation. The proposed security system consists of a smart device equipped with Android 2.2 and a Java based security server.

To evaluate the convenience of our system, we experimented our system in a network environment with diverse time and location. As a result, when the context information which is analyzed at the time of login does not agree with the existing access pattern, additional authentication is requested, and the average access pattern and the security level are automatically controlled and updated. The administrator can configure security environment automatically without any operation. Also the proposed system provides convenience. By applying the SEED algorithm to data it not only protects itself from sniffing and traffic capture attack with data encryption but also provides confidentiality and privacy.

Finally to evaluate the system efficiency, experiments were condeucted in three test cases as shown in Fig. 5. The there test cases are (1) applying only ID/PW, (2) applying ID/PW and additional authentication always, and (3) applying ID/PW and additional authentication contextually.

Fig. 6 shows the amounts of RAM and CPU used in each test environment. These tests were conducted in various locations, times and network environments. Especially, the tests of the proposed contextually additional authentication system were conducted (1) in the context identical to all the access patterns of the user, (2) in the context where only particular parts of the pattern are identical, and (3) in the context where all the access patterns are different. As illustrated in Fig. 5, the context information based authentication system has a higher system efficiency than the environment which always requires basic authentication and additional authentication. Our system resolved problem of communication number increase between smart device and security server in additional process. Therefore it reduces RAM and CPU occupation. Although the system which requires only the basic authentication without requiring additional authentication has a higher system efficiency, it is liable to ID/Password leakage and undesirable device security issues such as losses and misplacements of the device.

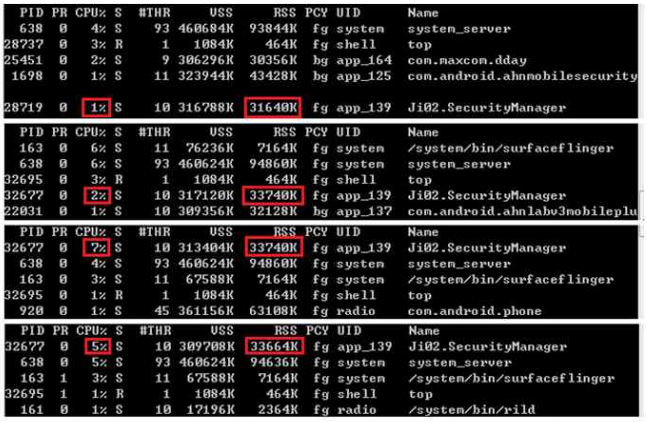
Table 7 shows result of test comparative analysis.

5. CONCLUSION

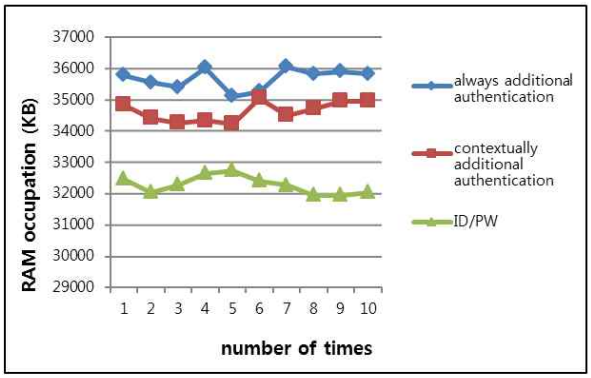
In this paper, we proposed a context-based authentication system which uses context information as well as ID/password for proper security services in the mobile device environment, and the validity of the proposed security system was successfully verified. The new context based

	Case of Test	Description
	ID/PW	Applying only ID/PW
	ID/PW + Additional authentication	Applying ID/PW and additional authentication always
○	ID/PW + Additional authentication	Applying ID/PW and additional authentication contextually

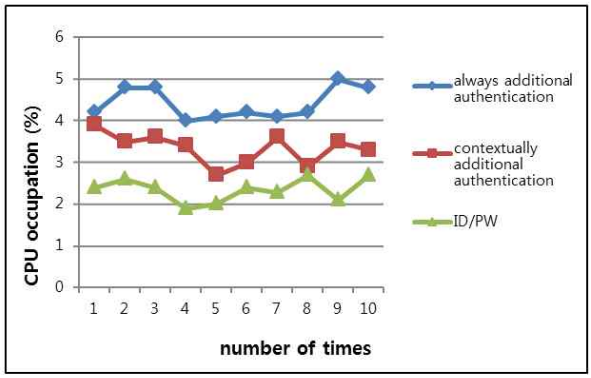
Fig. 5. Test Cases.



(a) RAM and CPU usages using 'top' command



(b) RAM occupation



(c) CPU occupation

Fig. 6. Comparisons of RAM and CPU Occupation.

authentication system resolves the problem of performance deterioration and offers more reliable accurate security than the existing simple ID/password based authentication system. In addition, we developed an optimization process which utilizes the fuzzy algorithm based user's estimation grade,

Table 7. result of test comparative analysis

	ID/PW	always additional authentication	contextually additional authentication
Usability	easy to access for mobile office → excellent usability	· User-focused: cause inconveniences (proposed additional authentication always) · Administrator-focused: decrease of inconveniences (manually operated security configuration)	· User-focused: proper conveniences (context based additional authentication) · Administrator-focused: improve conveniences (modification security configuration automatically)
Security	exposure of device security issues	difficult to access for mobile office (proposed additional authentication always)	· more difficult to access for mobile office than only ID/PW authentication system · applied data encryption → prove security defend sniffing attack and traffic capture
Efficiency	higher system efficiency	performance deterioration (Fig. 6)	reduces CPU and RAM occupation (additional authentication contextually) (Fig. 6)

intrusion detection, and risk of intrusion. We confirmed that the context information based authentication system has a higher system efficiency than the system which always requires basic authentication and additional authentication. Although the system which requires only the basic authentication without requiring additional authentication has a higher system efficiency, it is liable to ID/Password leakage and undesirable device security issues such as losses and misplacements of the device. In the future, we will analyze the defects and limitations of the proposed context based authentication system in actual field tests at the industry field. Further research will focus on the performance improvement and algorithm optimization for the proposed security system.

REFERENCES

[1] S.Y. Na. Y.H. Lee, S.j. Ji., "Smartphones and Mobile Office Security Issues and Strategies," *National Information Society Agency,* Vol. 26, No. 1, pp. 12-20, 2010.

[2] Gaeil An, Guntae Bae, Kiyoung Kim, and Dongil Seo, "Context-aware Dynamic Security Configuration for Mobile Communication Device," *Proc. of the Mobility and Security (NTMS 2009)*, pp.79-83 , 2009.

[3] Schilit. B., Adams. N., and Want. R., "Context-Aware Computing Applications," *Proc. of the 1st International Workshop on Mobile Computing Systems and Applications,* pp. 85-90, 1994.

[4] A.K. Dey, "Understanding and using Context," *Personal and Ubiquitous Computing J.,* Vol. 5, No. 1, pp. 4-7, 2001.

[5] Harry Chen, Tim Finin, Anupam Joshi, *An Intelligent Broker Architecture for Pervasive Context-aware Systems*, Doctorial Thesis of UMBC, 2004.

[6] Gaia project, http://gaia.cs.uiuc.edu, 2000.

[7] Tao Gu , Xiao Hang Wang , Hung Keng Pung ,Da Qing Zhang, "An Ontology-based Context Model in Intelligent Environments," *Proc. Communication Networks and Distributed Systems Modeling and Simulation Conference,* 2004.

[8] Hyun Kim, Young-Jo Cho, Sang-Rok Oh, "CAMUS - A Middleware Supporting Context-aware Services for Network- based Robots," *Proc. of IEEE Workshop on Advanced Robotics and Its Social Impacts, Nagoya*, pp. 237-242 , 2005.

[9] Jaegeol Yim, Gyeyoung Lee, Kyubark Shim, Thanh Cong Le., "A Method of Determining Whether a Smart-Phone is Moving," *Journal of Korea Multimedia Society,* Vol. 15, No. 5, pp. 632-638, 2012.

[10] Choi Sung-Min, Lim Jong-Kwon, Oh Sang-Keun, and SeoChee-Ho, "A Research for Weight Decision of Waterproofing Methods Selection Evaluation Item using the AHP," *Proceeding of The Korea Institute of Building Construction Conference,* Vol. 8, No. 2, pp. 205- 211, 2008.

[11] Satty, *T.L, The Analytic Hierachy Process*, McGraw Hill, America, 1980.

[12] L.A. Zadeh, "The Concept of Lingustic Variable and Its Application to Approximate Reasoning," *Infomation Sciences,* Vol. 9, No, 1, pp. 43-80, 1975.

[13] Hyung-Kwang Lee and Gil-Rok Oh, *Fuzzy Theory and Application, 1st Ed,* Hongreung Media, Republic of Korea, 1991.

[14] CVE: http://www.cve.mitre.org, 2012.

[15] Yong-Hyuk Kim, *Artificial Intelligence*, 2nd Ed, Hanbit Media, Republic of Korea, 2011.

[16] Da Young Chang, "Applications of the Extent Analysis Method on Fuzzy AHP," *European Journal of Operational Research,* Vol. 95, No. 3, pp. 649-655, 1996.

Jiyoung Yang

2011: BS in Computer Engineering, Education Center of Dongseo University
2011~Present: MS Candidate, Computer Engineering, Pukyong National University
Research Interests: computer security for application, context aware computing

Hyundong Lee

2001: BS in Computer Engineering, Kyungsung University
2007: MS in Computer Engineering, Pukyong National University
2012: Ph.D in Computer Engineering, Pukyong National University
Research Interests: computer security for application, context aware computing, RFID/USN/RTLS

Shi-Kook Rhyoo

1980: BS in Electronic Engineering, Kyungpook National University
1989: MS in Electronic Engineering, Yeungnam University
1997: Ph.D in Computer Science, Gyeongsang National University
1980~Present: Professor, Division of Info. Tech., Kyungnam College of Information & Technology
Research Interests: object-oriented database, multimedia, parallel processing

Mokdong Chung

1981: BS in Computer Engineering, Kyungpook National University
1983: MS in Computer Engineering, Seoul National University
1990: Ph.D in Computer Engineering, Seoul National University
1985~1996: Professor, Department of Computer Engineering, Pusan University of Foreign Studies
1996~Present: Professor, Department of Computer Engineering, Pukyong National University
Research Interests: OOP technology, computer security for application, intelligent agent, context aware computing