Context-Aware Security System for the Smart Phone-based M2M Service Environment

Hyundong Lee[1] and Mokdong Chung[2]
[1] Dept. of Computer Engineering, Pukyong National University, Korea
[e-mail: win4class@hanmail.net]
[2] Dept. of Computer Engineering, Pukyong National University, Korea
[e-mail: mdchung@pknu.ac.kr]
*Corresponding author: Mokdong Chung

Received September 2, 2011; accepted January 17, 2012; published January 31, 2012

Abstract

The number of smart phone users is rapidly growing due to recent increase in wireless Internet usage, development of a wide variety of applications, and activation of M2M (Machine to machine) services. Although the smart phone offers benefits of mobility and convenience, it also has serious security problems. To utilize M2M services in the smart phone, a flexible integrated authentication and access control facility is an essential requirement. To solve these problems, we propose a context-aware single sign-on and access control system that uses context-awareness, integrated authentication, access control, and an OSGi service platform in the smart phone environment. In addition, we recommend Fuzzy Logic and MAUT (Multi-Attribute Utility Theory) in handling diverse contexts properly as well as in determining the appropriate security level. We also propose a security system whose properties are flexible and convenient through a typical scenario in the smart phone environment. The proposed context-aware security system can provide a flexible, secure and seamless security service by adopting diverse contexts in the smart phone environment.

Keywords: Context-awareness, security, fuzzy logic, MAUT, M2M

This research was supported by Basic Science Research Program through the Nation-al Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2010-0024053).

DOI :10.3837/tiis.2012.01.004

1. Introduction

The number of smart phone users is sharply increasing these days due to the increase in demand for wireless internet, development of various applications, M2M (Machine to machine) services, and so on. A smart phone is a multi-functional mobile phone akin to a personal computer, providing not only a voice phone function, but also a variety of computer-like functions including email, internet, and e-book. While the smart phone provides outstanding mobility and convenience, security is one of its most frequently cited concerns, with a growing disquiet regarding its potential for leaking private information or causing direct financial damage to users [1].

Since most smart phones use simple ID and password-based authentication to verify user identity, users are obliged to create and manage a number of IDs and passwords for the many services they use, thereby causing complexity as well as inconvenience. Moreover, there is a security flaw caused by the loss and even theft of IDs and passwords. It is, therefore, essential that diverse multi-facts-based authentication and access control methods be implemented to solve the security issues.

This paper proposes a context-aware authentication system and an access control system, which verify the flexible and easy-to-use security systems for M2M services in the smart phone environment. In addition, this paper also conducts a comprehensive review of algorithms that analyze the contextual information of users, determining the security levels according to the contextual information.

The paper is organized as follows: Section 2 provides a review of relevant technologies applied to context-aware security systems; Section 3 offers information on the structure of context-aware security systems and a dynamic analysis of context information; Section 4 addresses the appropriate algorithms to determine security levels; Section 5 describes typical scenarios and an evaluation of proposed security systems; and Section 6 presents the results of the study and identifies possible directions for further research.

2. Related Work

2.1 Security Issues in the Smart Phone in the M2M Service Environment

Machine-to-Machine (M2M) communications denote the communication between two or more entities that do not necessarily need any direct human intervention. M2M services are designed to automate decisions and communication processes[2][3].

Smart phones for the M2M service provide users with various functions including PC, camera, voice recorder and tethering. In addition, since it is very easy for anyone to create and distribute mobile contents in an open environment, various security threats have occurred, too [4]. Figure 1 shows the security issues in the smart phone in an M2M service environment.

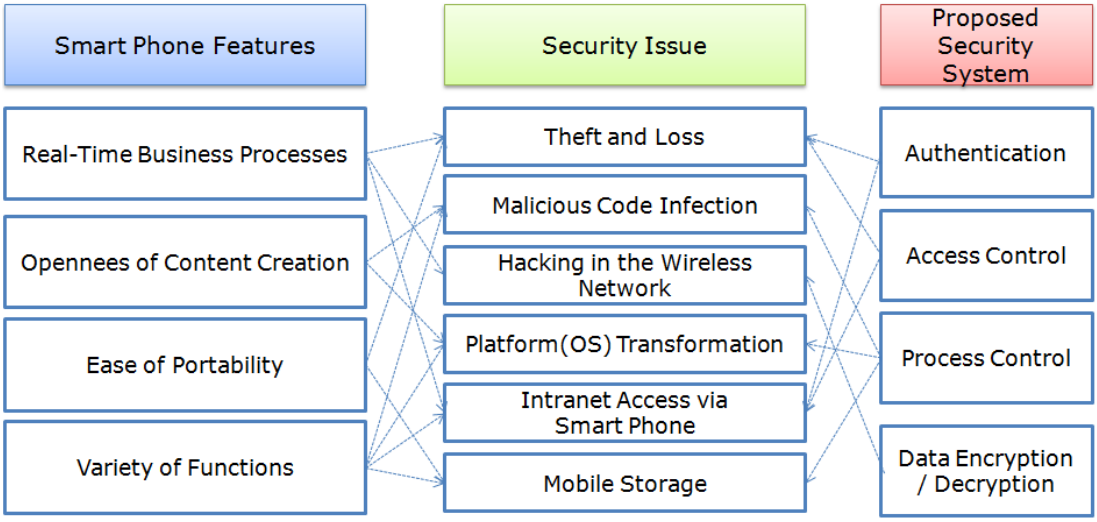

Fig. 1. Security issues in the smart phone in the M2M service environment.

2.2 Context-Aware Based Service

The first definition of context-aware[5] technology given by Schilit[6] is that "context-aware software adapts to the location of user, the collection of nearby people, hosts, and accessible devices, as well as to changes to such things over time."

Most research on context information processing (CoBra[7], Gaia[8], SOCAM[9], CAMUS[10]) is related to collecting information and providing service, but it is difficult to verify whether the inference is appropriate or not. Our proposed system is structured to flexibly select the contextual information and function in order to give relevant feedback during the operation of the context aware security service, thereby providing more appropriate security service.

2.3 Fuzzy and MAUT algorithms

Fuzzy algorithms use membership functions which define how much of the collected information is included in a set of certain status in order to analyze their context information[11]. The fuzzfied status of the context information "e" from the environment variable 'x' can be defined with the following formula.

$$fuzzification_{x}(e) = \sum_{s^x}^{\forall s^x} \mu_{s^x}(e)/s^x \tag{1}$$

where "s^x" refers to the status of the environment variable "x" and "$\mu_{s^x}(e)$" refers to the fuzzy membership function for the status (between 0 and 1).

MAUT (Multi-Attribute Utility Theory) is a systematic method that identifies and analyzes multiple variables to provide a common basis for arriving at a decision[12].

According to MAUT, the overall evaluation $u(x)$ of an object x is defined as a weighted addition of its evaluation with respect to its relevant value dimensions.

The common denominator of all these dimensions is the utility for the evaluator.

$$u(x_1, x_2, \ldots, x_n) = \sum_{i=0}^{n} k_i u_i(x_i), \quad \sum_{i=0}^{n} k_i = 1 \tag{2}$$

(k_i : weighting coefficient, $u_i(x_i)$: utility function for the property)

3. Context-Aware Integrated Security System

This section describes the features of the proposed Context-Aware integrated Security System. The context-aware algorithms are proposed in the next section.

3.1 Architecture of the Context-Aware Integrated Security System

The proposed Security Server consists of a Security Manager, Context-Aware Manager, and UI Manager. The smart phone also has a Security Manager and UI Manager for its clients. Figure 2 shows the general architecture of the Context-Aware security system.

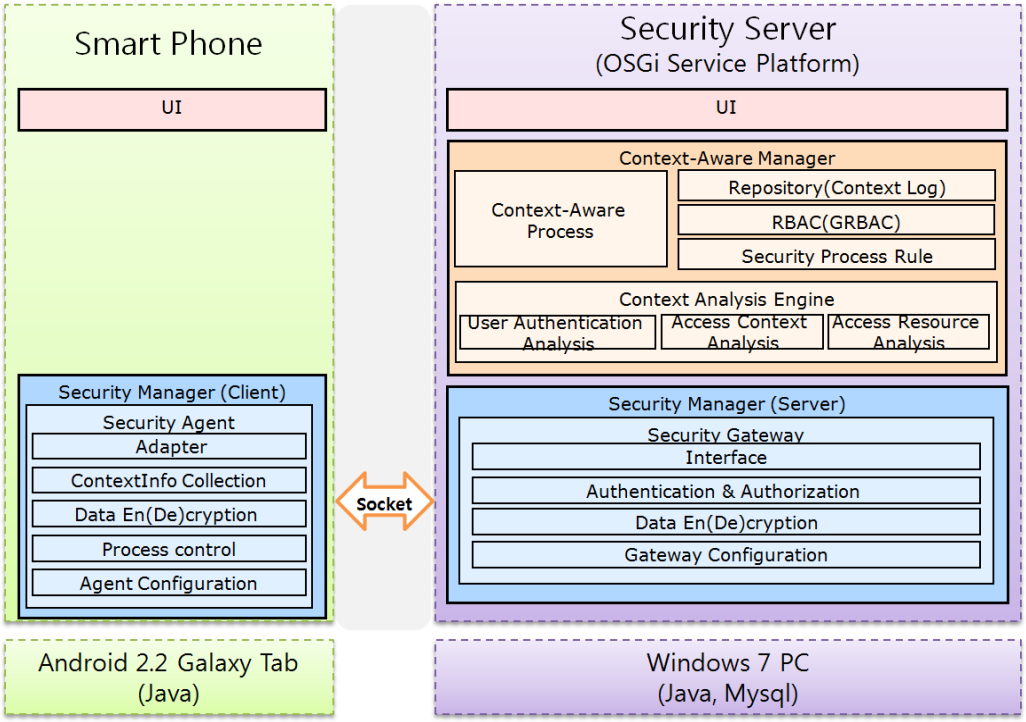

Fig. 2. Architecture of Context-Aware security system

3.1.1 Security Manager

The Security Manager uses a single form of authentication, and it consists of a Security Agent and Security Gateway in the smart phone environment. The Security Manager contains the following sub-modules:

- Security Agent: Security agent is installed in smart phones which run a user program, and it collects the user authentication information when users log into the system.
- Security Gateway: Security gateway is installed in the Security Server, and it processes user authentication with the user authentication information from the Security Agent.

3.1.2 Context-Aware Manager

The Context-Aware Manager performs a defining authentication process through diverse analyses of user authentication information based on the context. The Context-Aware Manager contains the following sub-modules:

- Context-Aware Process which is related to user permission, access context, and access resource. It makes inquiries about the context of the authentication process
- Repository which saves context information collected during user authentication, detects intrusion and saves response time
- RBAC(GRBAC)[13][14][15] which provides access control settings for each resource.
- Security Process Rule which defines user authentication procedures and roles.
- User Authentication Analyzer which analyzes the user's permission.
- Access Context Analyzer which analyzes user’s access network and time context.
- Access Resource Analyzer which analyzes access permission for the access resource.

3.1.3 UI Manager

The UI Manager provides smart phones with user authentication. It basically provides authentication of the UI-based ID Federation, and, in addition, OTP authentication UI according to context.

3.2 Data Flow between User and Security System

Examining the data flow between the smart phone user and Context-Aware security system, the Security Manager transfers to the Context-Aware Manager the information acquired while the user logs in from a smart phone, including user ID, IP address of the smart phone, resource information, IP address of the resource being accessed, and access time.

The Context-Aware Manager (Security Server) determines the security level based on the context information, then transfers to the Security Manager the information on authentication procedure and access control and process blocking . If the authentication is successful, the user can then gain access to information from M2M services, including RFID, IP-Camera, GPS and Sensor. Figure 3 shows the security data flow for M2M service environment.

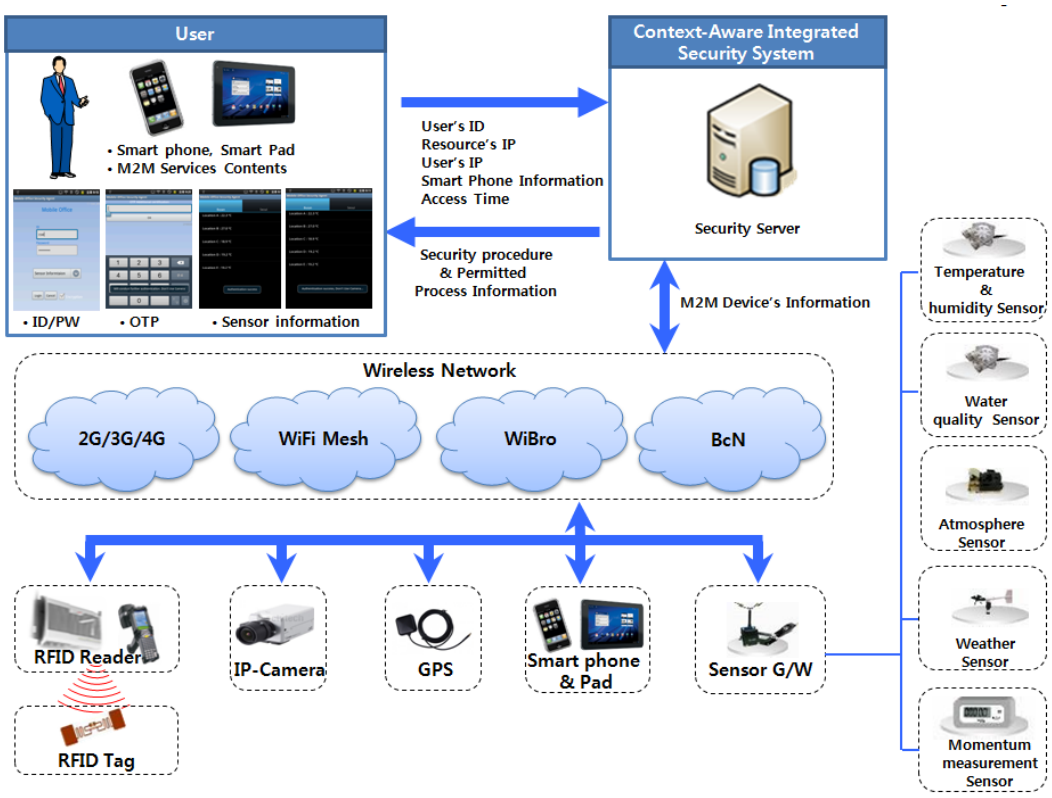

Fig. 3. Security data flow for an M2M service environment

Table 1 shows the context-aware integrated security system process.

Table 1. Context-aware integrated security system process

Notations	
ID_u	User Identification
PW_u	User password
$RESIP_u$	Resource's IP
$UserIP_u$	User's IP
$SmartphoneInfo_u$	Smart phone Information
$Time_u$	Access Time
SP_u	Security Procedure
$Process_u$	Process Information
Detailed Protocol	
(1) UI → Security Manager: ID_u//PW_u//ContextInfo($RESIP_u$,$UserIP_u$,$SmartphoneInfo_u$,$Time_u$) (2) Security Manager: Check[ID_u//PW_u] (3) Security Manager → Context-Aware Manager: ID_u//ResultofCheck[ID_u//PW_u]//ContextInfo($RESIP_u$,$UserIP_u$,$SmartphoneInfo_u$,$Time_u$) (4) Context-Aware Manager: Analysis[ID_u//ContextInfo($RESIP_u$,$UserIP_u$,$SmartphoneInfo_u$,$Time_u$)] (5) Context-Aware Manager → Security Manager: SP_u //$Process_u$ (6) Security Manager: Execute[$Process_u$] (7) Security Manager → UI: SP_u (8) UI: UI[SP_u]	

3.3 Dynamic Analysis of Context Information

The proposed Context-aware security system consists of OSGi service platform based bundles, which dynamically analyze the context information of each domain.

Dynamic analysis allows the system to lessen (decrease?) the system overhead owing to its flexible application of security service according to various domain statuses. Figure 4 illustrates the architecture of the domain based context information processing bundle.

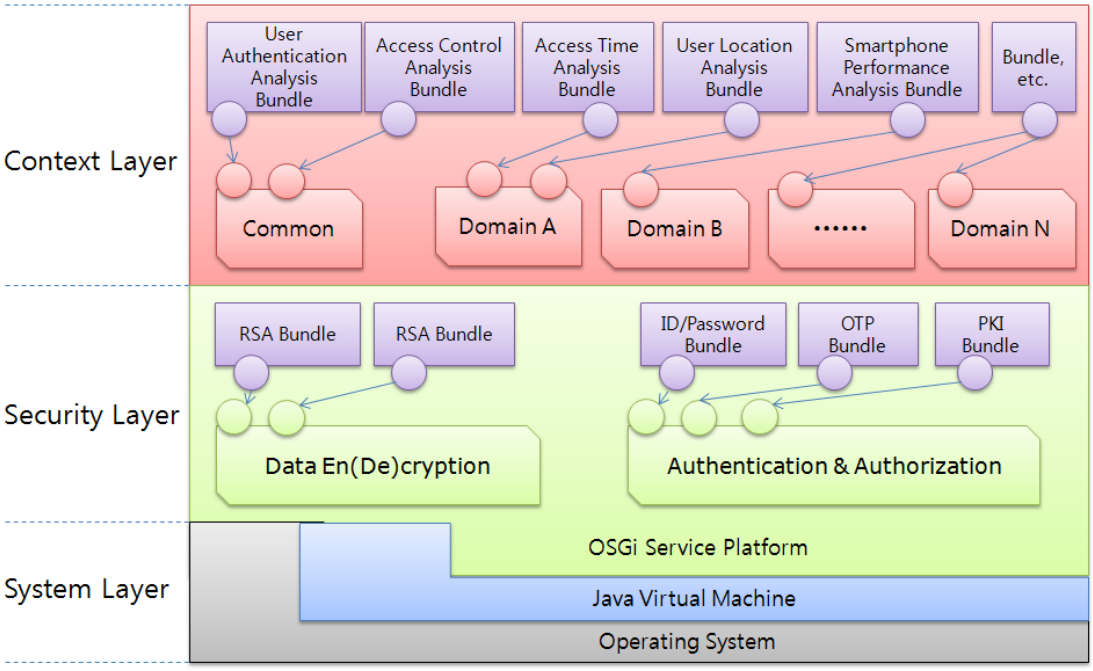

Fig. 4. Architecture of a domain based context information processing bundle.

This domain based context information processing bundle consists of a user permission analysis bundle and an access control analysis bundle which works at the beginning of the system's operation. Afterwards, the Security Manager dynamically analyzes the context information by adding context information bundles from the system environment configuration. Table 2 shows an example of how bundles can be used for each domain.

Table 2. Example of using Bundles for each different domain

Status	Default bundle	Additional bundle	Description
Default	User permission Access authority	NULL	Declare additional by analyzing user permission and access authority to the resource
Domain A	User permission Access authority	User location	In addition to basic user permission and access authority, this analyzes the user's location and determines the security level
Domain B	User permission Access authority	Device performance analysis	In addition to basic user permission and access authority, this analyzes the device performance and determines the security level

4. Algorithms to Determine Security Level

4.1 Overview

The context-aware security model proposed in this paper determines the security level on the basis of the context information generated by the analysis performed by MAUT algorithm and Fuzzy algorithms.

Moreover, this model verifies the security environment by using Fuzzy algorithms to optimize the security status. Figure 5 shows the procedures of context information analysis and security level determination.

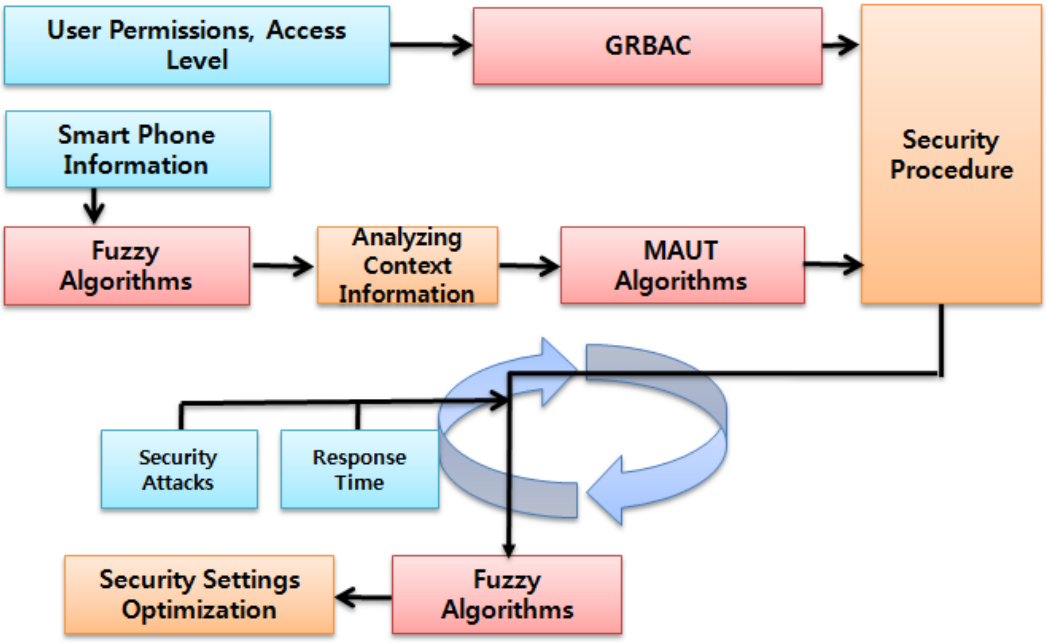

Fig. 5. The procedures of context information analysis and security level determination.

4.2 Fuzzy Algorithms for Context Information Processing

The fuzzy algorithm analyzes the context information acquired from user authentication on the smart phone. Since the context information acquired from user authentication is ambiguous when defining a certain status quantitatively, a fuzzy algorithm is used as the basic data to analyze the context information via quantitative estimation.

For instance, if a Fuzzy algorithm is applied to smart phone device information (CPU: 1Ghz, memory: 1Gbye, and battery charge: 90%), its performance could be estimated as ‘Good’.

Figure 6 shows the Fuzzy algorithm that analyzes the context information using Matlab.

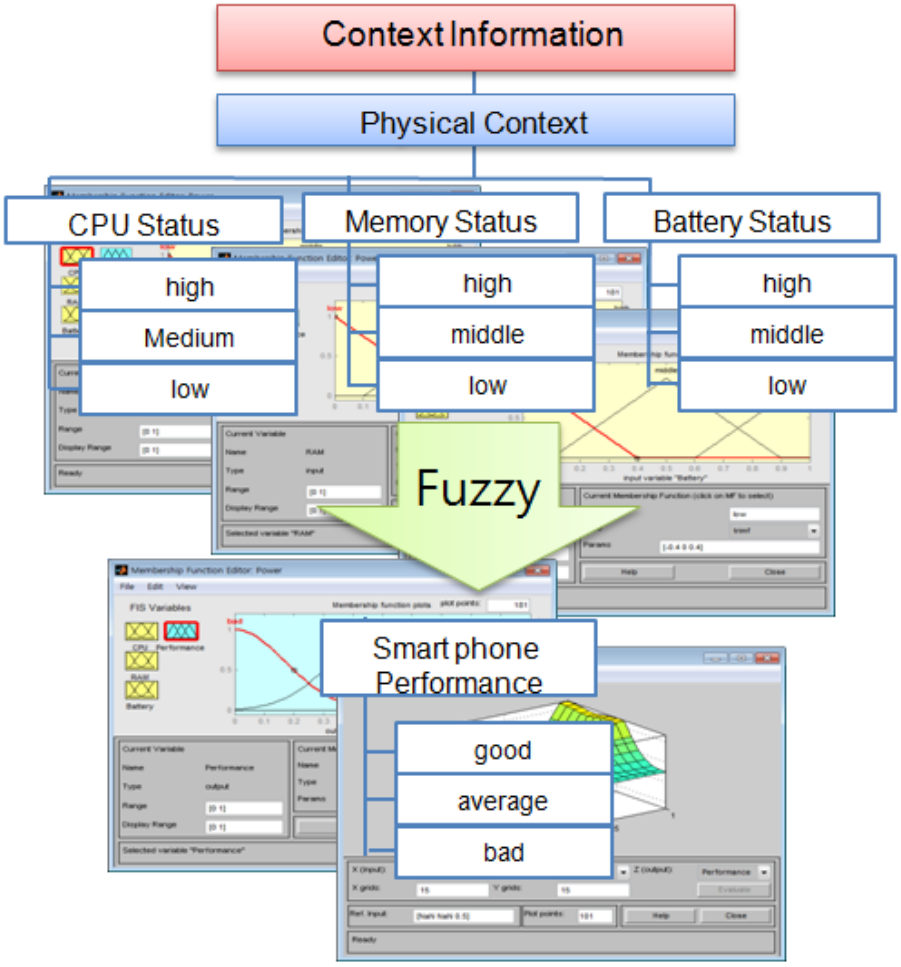

Fig. 6. The Fuzzy algorithm analyzing context information using Matlab.

When analyzing the device information without a Fuzzy algorithm, a large number of rules should be defined to assess whether the performance is good or not. Moreover, it is somewhat difficult to arrive at a quantitative analysis of a device performance. However, it is the flexibility of Fuzzy algorithm that enables the analysis of the device functions.

If the Security Manager modifies the security settings, a Fuzzy algorithm can verify the optimization of the security settings based on the cases of security attacks, and response time. In other words, after changing the security settings, the Fuzzy algorithm confirms the reasonability of the changed security settings based on repeated checking of security attacks and the response time. The feedback is then sent to the Security Manager.

4.3 MAUT Algorithm to Determine Security Level

An MAUT algorithm determines the security level based on context analysis data which has been generated by a Fuzzy algorithm. The strength of this method is that the MAUT algorithm determines the security level according to the importance of context information, not by simple rules.

Table 3 describes the MAUT algorithm. By multiplying each attribute of the context via Fuzzy algorithm by its weighting factor and comparing it with pre-defined security values, the MAUT algorithm determines the security value which is closest to the user's preference.

Table 3. Description of the MAUT Algorithm

MAUT(*X*)
for i = 1 **to** n
if *Repository* == *null* **then**
ask the user's preference and **decide** k_i**;**
else update k_i**;** //reference of repository*(User Location, Access Time)*
$u(x_1,x_2,\ldots,x_n) = k_1u_1(x_1)+k_2u_2(x_2)+\ldots+k_nu_n(x_n)$
// k_i: set of positive scaling constants for all *i*
// x_i: domain dependent variable, where $u_i(x^o_i)=0, u_i(x^*_i)=1$
do $u_i(x_i)$ = GetUtilFunction(x_i) **end**
if $u(x_1,x_2,\ldots,x_n) == u(x_{sp})$ **then**
return sp;
end;

GetUtilFunction (x_i)
// Determine utility function due to users' preferences
// x_i is one of domain dependent variables
uRiskProne : user is risk prone for x_i // convex
uRiskNeutral : user is risk neutral for x_i // linear
uRiskAverse : user is risk averse for x_i //concave
x: arbitrary chosen from x_i , *h*: arbitrary chosen amount
<*x*+*h*, *x*-*h*> : lottery from x+h to x-h
// where the lottery (x^*, *p*, x^o) yields a *p* chance at x^*
// and a (*1-p*) chance at *xo*
ask user to prefer <*x*+*h*, *x*-*h*> or *x* // interaction
if user prefer <*x*+*h*, *x*-*h*> **then**
return uRiskProne; // e.g. $u = b(2^{cx}-1)$
else if user prefer x **then**
return uRiskAverse; // e.g. $u = b\log_2(x+1)$
else
return uRiskNeutral;
end; // e.g. $u = b$

In the MAUT algorithm, the utility function '*u*' is determined as that of risk adverse, risk neutral, or risk prone [12].

- We ask the decision maker if he or she prefers <x+h, x-h> or x for arbitrarily chosen amounts of x and h.
- If he or she prefers the lottery, then we have a reason to believe that he or she might be risk prone
- If he or she prefers the expected consequence x, then we can believe that he or she might be risk averse
- The same question should be repeated using different amounts of either x or h.

Unless an MAUT algorithm is applied to determine the security level, we would have to adopt the same weighting value when determining the security level even though there are serious differences between the weighting factors to provide the appropriate security service.

5. Scenarios and Evaluation of the Proposed Security System

5.1 Scenarios in Each Phase

A user tries default authentication (ID and password) to access an M2M service via his or her smart phone.

The security server analyzes the information of the authentication and context data, and notifies the user of the authentication such as 'Authentication succeeded', 'Additional authentication request' or 'Service denied'.

The scenario for the proposed security system consists of an initial setting phase, which is configured when introducing the security system, a security system operation phase, and a security setting optimization phase. Table 4 shows the context information of each user in applying the scenario.

Table 4. The context information of each user in applying the scenario

User	Context Information
User A	▪User's ID: user1 ▪Resource's IP: 203.250.123,180 ▪User's IP: 202.250.123,100 ▪Access Time: 09:00:00 ▪Smart phone Information: -CPU: 1Ghz, RAM: 1Gbyte, Battery: 90%
User B	▪User's ID: user2 ▪Resource's IP: 203.250.123,190 ▪User's IP: 202.30.34.2 ▪Access Time: 09:00:00 ▪Smart phone Information: -CPU: 600Mhz, RAM: 512Mbyte, Battery: 80%
User C	▪User's ID: user2 ▪Resource's IP: 203.250.123,190 ▪User's IP: 202.30.34.2 ▪Access Time: 07:00:00 ▪Smart phone Information: -CPU: 600Mhz, RAM: 512Mbyte, Battery: 10%
User D	▪User's ID: user2 ▪Resource's IP: 203.250.123,190 ▪User's IP: 202.30.34.2 ▪Access Time: 07:00:00 ▪Smart phone Information: -CPU: 600Mhz, RAM: 512Mbyte, Battery: 80%
User E	▪User's ID: user1 ▪Resource's IP: 203.250.123,190 ▪User's IP: 202.30.34.2 ▪Access Time: 07:00:00 ▪Smart phone Information: -CPU: 600Mhz, RAM: 512Mbyte, Battery: 80%

1) Initial Setting Phase

① Security Manager configures the initial settings for the security system.

▪Select context information bundle(s)
-Select default bundle: User Authentication Analysis Bundle, Access Control Analysis Bundle
-Additional bundle(s): Smart phone Performance Analysis Bundle, User Location Analysis Bundle, Access time Analysis Bundle

▪Specify authentication procedure and access permission by security level

Context Information & Value	Definition
User location + Access time ≥ 0.5	ID and password authentication succeeds, all process
User location + Access time < 0.5	request additional authentication(OTP), Can't use the camera-related processes
Smartphone performance < 0.5	deny access

▪Specify default response time

-Default response time: response time after security service is applied – response time when security service is not applied = 0.1ms

▪Specify encryption/decryption algorithm for initial data(Level)

Encryption/decryption algorithm	Selection
Apply non	X
AES	O
RSA	X

2) Security System Operation Phase

① When loading the authentication window, the Security Agent in the smart phone retrieves the necessary context information and data encryption/decryption information from the security server.

Request of Context Information	Encryption/decryption algorithm
▪Default context information: User permissions and access right of the resource ▪Additional context information: Smart phone Information(CPU, RAM, Battery Status), User Location, Access Time	AES

② Collect the basic information for authentication (ID and password) and the context information, encrypt it using predefined encryption algorithm, and then transfer it to the security server.

▪ Collect user information, encrypt it using AES, and then transfer it to the Security Gateway in the security server.

③ The Security Server decrypts the data and verifies whether the ID and password are correct or not.

• If the authentication fails, it requests another authentication attempt from the user.

▪ Decrypt data using AES, and verify the ID and password.
If the ID or password is incorrect, print out 'Login error' to user and make a request for ID and password authentication.

• If the authentication succeeds, it requests the Context-Aware Manager for context information analysis.

④ After completing the context information analysis by using a Fuzzy algorithm and the user permission analysis, the security system hen determines the security level by applying the MAUT algorithm.

Figure 7 and steps_ⓐ, ⓑ, ⓒ indicate the procedure for security level determination.

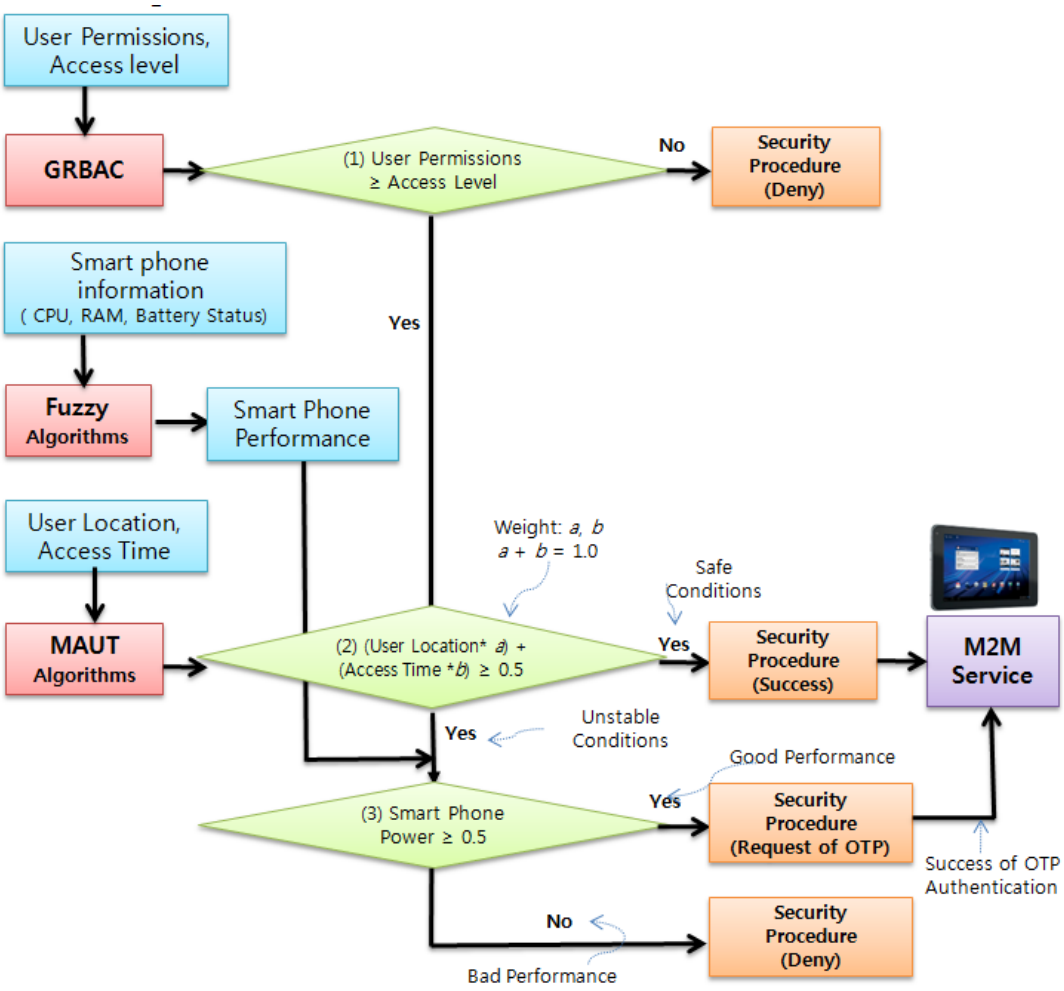

Fig. 7. Security level decision-making process.

Step_ⓐ Compare and analyze user permissions and access authority of the resource. If user permission is lower than access authority of the resource, deny the access.

▪Compare user permissions and access right of the resource by analyzing the user ID and IP address of the resource to be accessed.
▪If user permission is greater than or equal to the access right of the resource, connect to the service. Otherwise, deny access.

Permission	Classification	Value
User Permissions	Guest	0.00
	User	0.50
	Admin	1.00
Access Level	Low	0.00
	Middle	0.50
	High	1.00

User	User permissions and access right of the resource	Analysis
User A	▪User's ID: user1 (user) ▪Resource's IP: 203.250.123,180 (Low)	user permission(0.5) > access right of the resource(0.0) →connect to the service

User B	▪User's ID: user2 (admin) ▪ Resource's IP: 203.250.123,190 (High)	user permission(1.0) = access right of the resource(1.0) → connect to the service
User C	▪User's: user2 (admin) ▪ Resource's IP: 203.250.123,190 (High)	user permission(1.0) = access right of the resource(1.0) →connect to the service
User D	▪User's: user2 (admin) ▪ Resource's IP: 203.250.123,190 (High)	user permission(1.0) = access right of the resource(1.0) →connect to the service
User E	▪User's: user1 (user) ▪ Resource's IP: 203.250.123,190 (High)	user permission(0.5) < access right of the resource(1.0) → deny access

Step_ⓑ Context-Aware Manager analyzes context information by using a Fuzzy algorithm.

▪Analyze performance of the smart phone device using a Fuzzy algorithm based on device information (CPU: 1Ghz, memory: 1GByte, and battery charge: 90%)
▪Input variable: CPU(low, middle, high), RAM(low, middle, high), Battery(low, middle, high)
▪Output variable: Performance(bad, average, good)
▪Rules:
1. If (CPU is low) and (RAM is low) and (Battery is low) then (Performance is bad)
< Skip>
27. If (CPU is high) and (RAM is high) and (Battery is high) then (Performance is good)

Step_ⓒ the Context-Aware Manager collects the analyzed context information and determines the security level by using the MAUT algorithm.

▪After analyzing the context information, collect the results and determine security level.

Context Information	Classification	Value
User Location	Outside	0.00
	Branch office	0.25
	Head office	0.50
Access Time	Off hour	0.00
	Working hour	0.50
Smart phone performance	Bad	0.00
	Average	0.50
	Good	1.00

▪If user location and access time exceed 0.0, request additional authentication (OTP). If it is more than 0.5, ID and password authentication have been successful.

User	Context Information (User Location, Access time)	Analysis
User A	▪User's IP: 202.250.123,100 ▪Access Time: 09:00:00	▪User Location: Head office (0.50) ▪Access time: working hour (0.50) → 1.00: ID and password authentication succeeds
User B	▪ User's IP: 202.30.34.2 ▪ Access Time: 09:00:00	▪User Location: Outside (0.00) ▪Access time: working hour (0.50) → 0.50: ID and password authentication succeeds
User C	▪ User's IP: 202.30.34.2 ▪ Access Time: 07:00:00	▪User Location: Outside (0.00) ▪Access time: off hour (0.00) → 0.00: request additional authentication (OTP)
User D	▪ User's IP: 202.30.34.2 ▪ Access Time: 07:00:00	▪User Location: Outside (0.00) ▪Access time: off hour (0.00) → 0.00: request additional authentication (OTP)

▪In the case of a request for additional authentication (OTP), a smart phone with low performance cannot proceed with additional authentication; therefore, access from smart phones with performance value under 0.5 will be denied.

User	Context Information (smart phone performance)	Analysis
User A	▪smart phone performance: -CPU Status: 1Ghz -RAM Status: 1Gbyte -Battery Status: 90%	▪smart phone performance : Good (1.00) → 1.00: ID and password authentication succeeds
User B	▪smart phone performance: -CPU Status: 600Mhz -RAM Status: 512Mbyte -Battery Status: 80%	▪smart phone performance : Average (0.50) → 0.50: ID and password authentication succeeds
User C	▪smart phone performance: -CPU Status: 600Mhz -RAM Status: 512Mbyte -Battery Status: 10%	▪smart phone performance : Bad(0.00) → 0.00: deny access
User D	▪smart phone performance: -CPU Status: 600Mhz -RAM Status: 512Mbyte -Battery Status: 80%	▪smart phone performance : Average (0.50) → 0.50: request additional authentication (OTP)

⑤ In accordance with the security level, encrypt the security procedure and information of the permitted process, and transfer it to the Security Agent in the smart phone.

▪Encrypt the security procedure and permitted process information using AES and transfer it to the Security Agent in the smart phone.

User	Security procedure	Permitted process information
User A	authentication succeeds	all processes
User B	authentication succeeds	all processes
User C	deny access	-
User D	request additional authentication(OTP)	Can't use the camera-related processes
User E	deny access	-

⑥ The Security Agent decrypts the data, identifies the security procedure and permits the process, and then provides services.

- When the authentication succeeds, only the permitted process can work during the service.
- If any additional authentication such as OTP and PKI is requested, try additional authentication.

3) Security Setting Optimization Phase

While operating the security system, if there is an increase in security attacks and intrusions, thus a slowdown in the response time, make a request to the administrator to adjust the security settings. After the Security Manager has adjusted the settings, verify the security settings using a Fuzzy algorithm, and then complete the security settings. Figure 8 shows the optimization procedure for security settings.

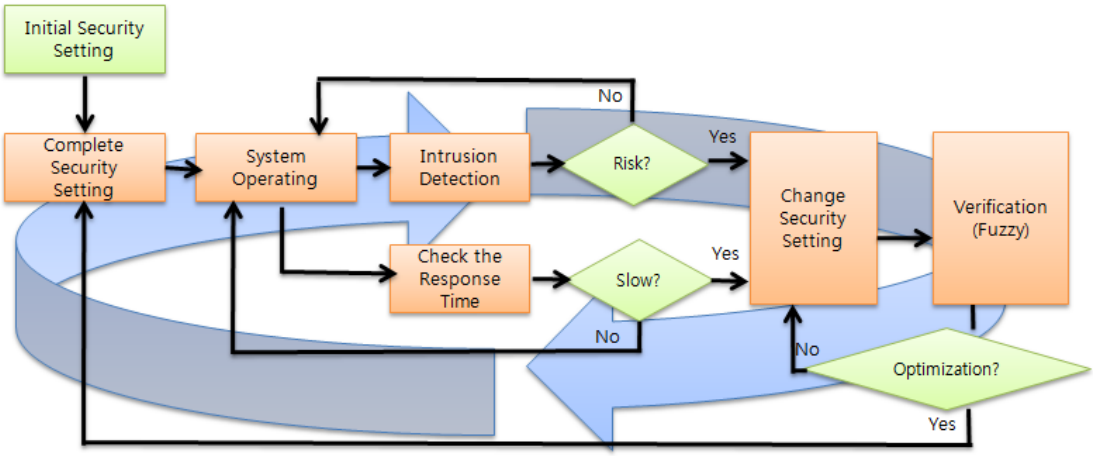

Fig. 8. The optimization procedure for security settings.

① Detect unauthorized accesses, measure the response time and store it in a repository of the security server.

② In the case of an increase in the number of security attacks and intrusions, and thus a slowdown in the response time, make a request to the administrator to adjust the security settings.

▪ If any threat to a users device occurs, request that the Security Manager enhance the process control
▪If any threat occurs in a wireless network, request that the Security Manager enhance the encryption/decryption level (e.g. AES to RSA)
▪If any threat to service occurs, request that the Security Manager enhance authentication and access control
▪If system response time slows down, request that the Security Manager enhance the encryption/decryption level for context information analysis bundle(s)

③ Once the security settings are adjusted by the Security Manager, verify the security setting optimization using a Fuzzy algorithm, and then send feedback to the Security Manager such as 'Remain at current settings', 'Set higher security settings' and 'Set lower security settings'.

▪ Input variable: Security(Perfect, Allow, Risk),
Performance(Fast, Normal, Slow)
▪Output variable: Security Level (Upward, NoChange, Downward)
▪Rules:
1. If (Security is Perfect) and (Performance is Fast) then (Security Level is NoChange)
< Skip >
9. If (Security is Risk) and (Performance is Slow) then (Security Level is Upward)

5.2 Evaluation of The Proposed System

1) Problems Encountered by the Existing Systems

① When using an ID and password to access the M2M service on a smart phone, there is always the possibility of losing the ID and password or experiencing difficulty in managing many IDs and passwords for each service. The proposed system in this paper has adopted the Single Sign On (SSO) to resolve this issue.

② When users try to gain access to important resources with their IDs and passwords only, there is a high possibility of security threats, especially in the weak security environment. The proposed context-aware security system resolves these issues with its context-aware service, multi-fact authentication and RBAC-based access control.

2) Issues and Resolution of the Proposed System

① Introducing a security system may cause a high overhead over the entire system. The proposed system adopted an OSGi system platform to enable the manager to classify frequently used context information by each domain, and if necessary, dynamically configure the context information processing bundle(s) seamlessly without having to stop the system.

② For analyzing ambiguous context information of a smart phone user, a Fuzzy algorithm is applied to enable a quantitative analysis.

③ A weighting factor is required on more important information in order to determine the security level. For this purpose, the proposed system determines the security level (authentication methods and process control) by using the MAUT algorithm.

④ Once the security system settings are completed, it is necessary to verify that the settings are appropriate. To do that, the proposed system optimizes the security settings by applying a Fuzzy algorithm based on the cases of security breaches and response time.

⑤ The proposed Context-Aware Security System provides a wide variety of security services for the smart phone environment including integrated authentication (ID/password, OTP, and PKI) and RBAC- based access control services, and it also ensures data confidentiality and integrity in the smart phones as well as a server layer via data encryption and decryption. Moreover, the proposed system prevents the activation of malicious codes via process control when using important resources in the smart phone.

3) Benefits of the Proposed Security System

① When using an M2M service in a smart phone environment, the proposed system analyzes ambiguous user context (Fuzzy algorithm), determines security level (MAUT algorithm) and provides context-aware security service via optimized authentication, access control, and process control service.

② The proposed system improves on the efficiency of the existing security system through the dynamic configuration of context processing bundle(s) to process only the necessary context information.

③ The proposed system provides repeated feedback and a system optimization process based on the cases of security breaches and response time and retains the optimized security configuration.

4) Evaluation

Table 5 shows a comparison of a single authentication system and the proposed system in terms of the ISO9126 Quality Model, which is equipped with superior functionality, reliability, usability, efficiency, maintainability, and portability.

Table 5. Comparison between a single authentication system and the proposed system

Topics	Legacy System	proposed system
Functionality	Single authentication	Multi-factor authentication
Reliability	Patches when the system stops	Continuous authentication system
Usability	Fixed authentication service	Versatile and flexible authentication service
Efficiency	For diverse contexts, providing the same authentication	Providing appropriate authentication process to minimize the cost for certification
Maintainability	Patches when the system stops	Seamless authentication system
Portability	Operate in a single platform	Operate in multi platforms

Figure 9 shows the comparison of the performance evaluation between a single authentication system and the proposed system.

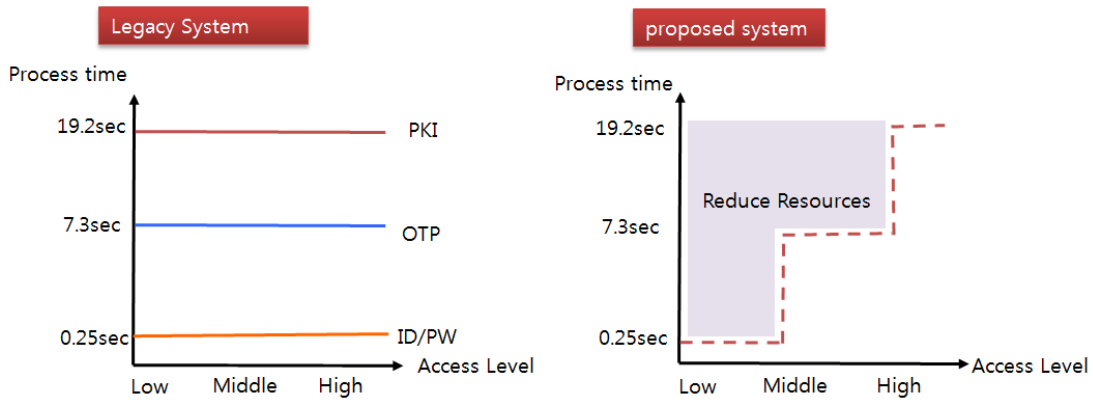

Fig. 9. Evaluation between a single authentication system and the proposed system.

6. Conclusion and Further Research

This paper proposed a context-aware authentication system which provides flexible and easy-to-use security systems for M2M services in the smart phone environment.

The key benefits of the proposed context-aware security system for smart phones are as follows:The Context-Aware Security System is able to

①Support various multi-facts based authentication procedures (ID/password based +OTP+PKI or access denial) and provide powerful authentication and access control, process control, and data encryption/decryption services.

②Dynamically add and delete context processing bundle(s) (OSGi service platform) while running the system. Essentially, this guarantees seamless security services.

③ Ensure high usability and system stability by providing diverse security services depending on user context via context analysis using Fuzzy, MAUT algorithms and security level determination.

Our future research will focus on the performance improvement and algorithm optimization for the proposed security system.

References

[1] KH. Nam. et al., "Smartphone security technology and solution trends," *Weekly Technical Trends, No. 1466*, pp. 1-7, 2010.

[2] ETSI TS 102 689 v1.1.1, "Machine-to-Machine communications(M2M); M2M service requirements," 2010.

[3] ETSI TS 102 690 v0.10.1, "Machine-to-Machine communications(M2M); M2M functional architecture," 2011.

[4] SY, Na. et al., "Smart phones and mobile office security issues and strategies," *National information society agency*, vol. 26, pp. 12-20, 2010.

[5] A. K. Dey, "Understanding and using context," *Personal and Ubiquitous Computing*, vol. 5, no. 1, pp. 4-7, 2001. Article (CrossRef Link)

[6] Schilit, B., Adams and N. Want, R., "Context-Aware computing applications," in *Proc. of the 1st International Workshop on mobile Computing Systems and Applications*, pp. 85-90, 1995. Article (CrossRef Link)

[7] H Chen, "An intelligent broker architecture for pervasive context-aware systems," *PhD thesis of UMBC*, 2004.

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

[9] Gu, T. et al., "An ontology-based context model in intelligent environments," in *Proc. of Communication Networks and Distributed Systems Modeling and Simulation Conference*, 2004.

[10] H. Kim et al., "CAMUS - A middleware supporting context-aware services for network-based robots," in *Proc. IEEE Workshop on Advanced Robotics and Its Social Impacts*, 2005.

[11] L. A. Zadeh, "Fuzzy sets," *Information and Control*, vol.8, pp. 338-353, 1965. Article (CrossRef Link)

[12] R. L. Keeney and H. Raiffa, "Decisions with Multiple Objectives: Preferences and Value Tradeoffs," *Cambridge university press*, pp . 261-271, 1993.

[13] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C.E.Youman, "Role-based access control models," *IEEE Computer*, vol. 29, no. 2, pp. 38 - 47, Feb. 1996. Article (CrossRef Link)

[14] M.J.Convington, M.J Moyer, and M.Ahamad, "Generalized role-based access control for Securing future applications," in *Proc of 23rd National Information Systems Security Conference (NISSC)*, pp. 115-125, 2000.

[15] M.J. Moyer and M.Ahamad, "Generalized Role-Based Access Control," in *Proc. of IEEE Int'l Conf. on Distributed Computing Systems (ICDSC2001)*, pp. 391-398, 2001. Article (CrossRef Link)

Hyundong Lee received a Ph.D. degree and an M.S degree in Computer Engineering from Pukyong National University in 2012 and in 2007, respectively.
His research interests are artificial intelligence and context-aware technology.

Mokdong Chung received a Ph.D. degree in Computer Engineering from Seoul National University in 1990. He was a professor at Pusan University of Foreign Studies from 1985 to 1996. And he has been a professor at Pukyong National University since 1996.
His research interests are OOP technology, computer security for application, intelligent agent, and context aware computing. He is a member of IEEE, KIISE, KIPS, KIISC, and KMMS.