International Journal of Smart Home
Vol.7, No.6 (2013), pp.91-100
http://dx.doi.org/10.14257/ijsh.2013.7.6.09

Implementation of Privacy Policy-based Protection System in BEMS based Smart Grid Service

Namje Park

Department of Computer Education, Teachers College, Jeju National University
namjepark@jejunu.ac.kr

Abstract

The fact that the information can be collected not only by the government and power companies but also individual users adds seriousness to the problem. In this paper examined this issue by focusing on the load management system based on BEMS that uses the privacy policy-based protection system in the smart grid environment. The structure of the privacy policy-based protection system using load management system in the smart grid environment is the structure that serves data in the load management system to the web through the application service network. For this, the privacy policy-based protection system suggested and developed the smart grid privacy policy-based protection system which controls service access by protecting items related to the personal information of the user and setting the privacy protection level for each item.

Keywords: *Smart Grid, BEMS, Privacy Protection, Policy, Privacy, Security*

1. Introduction

Smart Grid is the next-generation intelligent power network which optimizes energy efficiency through the mutual real time exchange of information between power supplier and consumer through the integration of existing power network and the information technology (IT). However, the smart grid environment can have problems involved with personal privacy invasion. For instance, if the network has the information about the devices that individuals have, the personal information is not saved to such devices but it can still cause a variety of cases of privacy invasion such as the information about whether the consumer is inside or outside his/her house based on the data about power consumption by year, month, date, and time zone that became available through the information of devices. The fact that the information can be collected not only by the government and power companies but also individual users adds seriousness to the problem. This paper examined this issue by focusing on the load management system based on BEMS (Building Energy Management System) that uses the privacy policy-based protection system in the smart grid environment. The structure of the privacy policy-based protection system using load management system in the smart grid environment is the structure that serves data in the load management system to the web through the application service network. For this, the privacy policy-based protection system suggested and developed the smart grid privacy policy-based protection system which controls service access by protecting items related to the personal information of the user and setting the privacy protection level for each item. Also, it analyzes the outcomes of smart grid privacy policy-based protection system. By applying smart grid privacy policy-based protection system, the user can show his/her information to the users requesting for such information through the mobile device or PC based on the privacy level he/she personally set and the information related with the device or to the users he/she designate and also receive

ISSN: 1975-4094 IJSH

the information he/she wants when he/she wants the information. By using this system, the company providing application services will be able to protect the personal information and become a reliable company and provide the service the user wants based on the information collected, expecting greater sales. Chapter 2 examines the need for personal information and the personal information protection in the smart grid and Chapter 3 provides the overview of the load management system and explains its structure, function, and database generation process. Chapter 4 examines the structure, function, and the creation mechanism of privacy policy-based protection system and explains the smart grid privacy policy-based protection system in connection with the contents discussed in Chapter 3 and the privacy policy-based protection system, and Chapter 5 provides the conclusion.

2. Design of Policy-based Privacy Protection System

2.1. Overview of Policy-based Protection

The privacy policy-based protection system is a service where the user who owns the information provides the mechanism for protecting his/her privacy. It is composed of the privacy policy-based protection system which manages the user's privacy protection policy, the system which determines the privacy policy of the user and sends this to the privacy policy-based protection system, and the system which provides information based on user's privacy protection policy.

2.2. Privacy Policy-based Protection Structure

When the user requests for the information he/she wants through the web using PC and mobile device, the service gate requests the directory server for the location of the information the user requests form. The directory server sends the URL address of the information application server which has the information to the user's PC or mobile device through the service gateway. When the user accesses the URL address, the information application server checks the privacy level authority of the user with the privacy server and shows the information available to the user based on the user's access level.

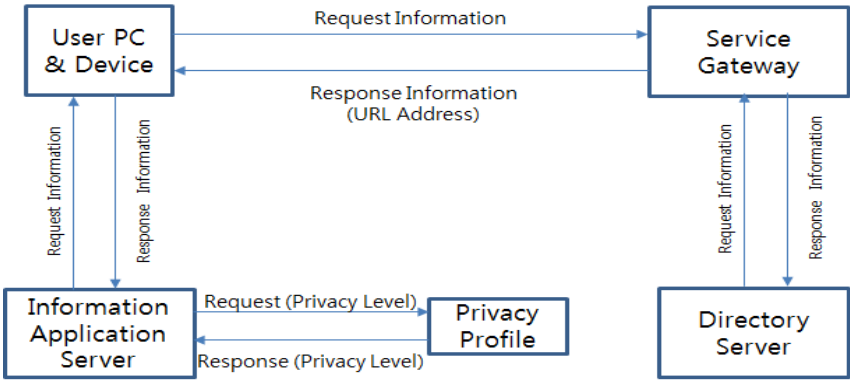


Figure 1. Privacy Policy-based Protection Block Diagram

2.3. Privacy Policy-based Basic Protection Function

The privacy policy based protection system managed by integration server provides different services through the administrator and the user. The administrator can register and

modify initial privacy, and the general user can register and modify user privacy and also register and modify access group.

2.4. Details of Privacy Policy-Based Protection System Functions

2.4.1. Administrator

User Registration: Information application server administrator can choose to register the privacy server or not when registering information application server to the directory server and register a user as the privacy server user by entering the IP and port of the corresponding privacy server. When registering a general user to the information application server the information of the general user is registered to the privacy server to which the information application server administrator is registered as a user. The user can use the privacy function by logging on to the web manager provided by the integration server with the ID and password he/she used to register to information application server.

Initial Registration and Modification of Privacy: Information application server administrator can set the privacy level for the item about the page to authorize through the information application server by logging on to the web manager provided by the integration server to which the privacy server is registered as user, or modify previously set level. This is called initial privacy setting.

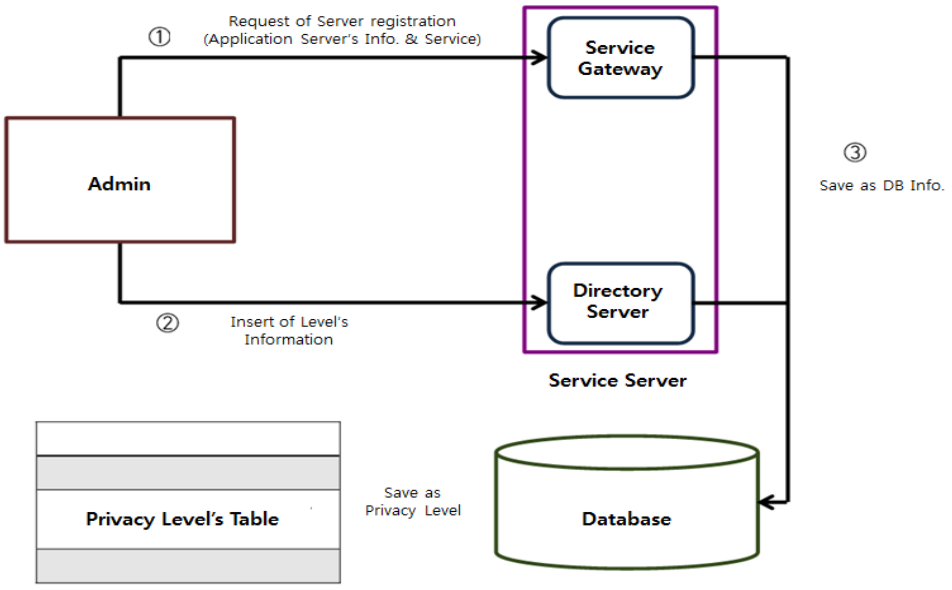


Figure 2. Privacy Policy-based Protection Function Flow

The following is the example for the configuration of the initial privacy for a service. In Figure 3, the items for a page provided by the information application server are as follows, and when a third party user accesses the connection information of the owner, the privacy policy-based protection system must provide only the information elements that take value equal to or less than (maximum privacy level – initial privacy level). In Figure 13, the basic privacy level is 5 and the third party can only access level 4 (9 - 5 = 4) or lower level item information.

Figure 3. Initial Privacy Set

2.4.2. User

User Registration: When a general user is registered to the information application server, the information of the general user is also registered to the privacy server to which the information application server administrator is registered as the user. The user can use privacy policy oriented fundamental protection function by logging on to the web manager provided by the integration server with the ID and password he/she used to register to information application server.

Registration and Modification of User Privacy: The general user registered as a user to the privacy server can log onto the web manager provided by the integration server to inquire about the registered information application list and also reset the privacy level for the items registered to the corresponding information application server. This is called user privacy setting, which is similar to the initial privacy described above.

2.4.3. Registration and Modification of Access Group

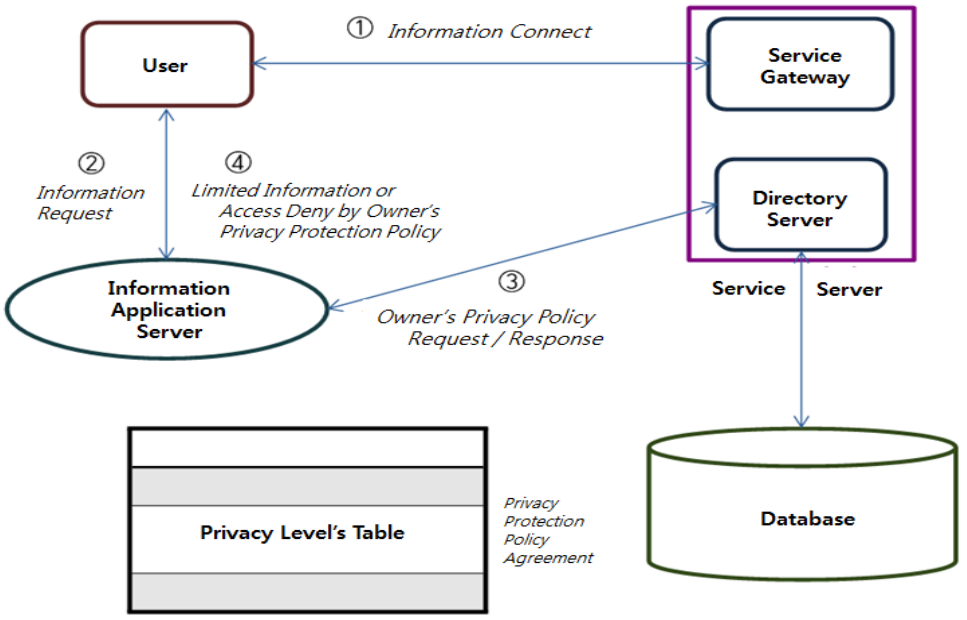
A general user registered as a user to the privacy server can log onto the web manager provided by the integration server and configure the access group for the information. The user can enter the mobile number for which he/she would set the privacy level to an access group and set initial privacy level as the access group when the third mobile number that he/she did not enter requests for information. The information request from mobile user carries out information access control similarly to administrator privacy interpretation. In other words, when the user in Access Group 4 requests for information, he/she can only access privacy level 5 (9 - 4 = 5) or lower level items.

Figure 4. Access Group Set

2.4.4. Information Inquiry based on Privacy Level

When the user connects to integration server by reading the code with a mobile device or PC, the integration server finds and links the user to the information application server to which the code is registered, and the user connects to the corresponding information application server. If the information provided by the information application server is

presented in the page to which the privacy level is applied, the server checks whether the number of the mobile device which requested for the access to privacy server is registered to the access group and allows only the number included in the access group. If the mobile number is not registered, the access is give according to the privacy level personally configured by the owner, and when the privacy level is not registered, the information access is controlled based on the initial privacy level registered by the administrator.



Figire 5. Information Reference Function According to the Privacy Level

3. Development of Privacy Protection System

In this paper, creation mechanism for initial privacy, user privacy, and access group based on privacy policy-based protection are as follows.

3.1. Initial Privacy Creation Mechanism

Initial privacy is created based on the initial privacy policy which defines the privacy policy, the item that exists in each service, by combining initial privacy policy and the administrator's information application schema. The example that uses this mechanism is presented in Figure 6.

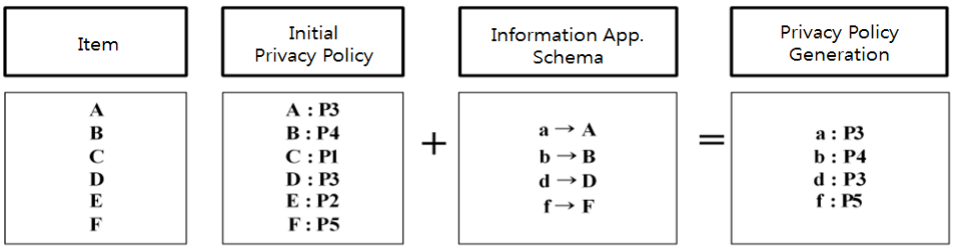


Figure 6. Initial Privacy Generation Mechanism

The item lists the type of information handled by each service group and the initial privacy policy provides basic privacy level recommended by the certificate authorities depending on information type, and this value is represented by the combination of the letter "P" and the number. Higher number indicates that the privacy must be protected more intensively. The information application schema is the list of the types of information that the administrator handles among the information handled by the item, and the administrator must map the information he/she handles with the information listed in the item. The type of information handled in this example is labeled with lower case English letter, and is mapped one-to-one with the information in the item to form the information application schema. A unique initial privacy can be created by using information application schema and initial privacy policy.

3.2. User Privacy Creation Mechanism

Like initial privacy, user privacy is created based on the initial privacy policy. First, the list of infoprmation handled enumerated by initial privacy policy and the default privacy level for information is suggested to the user. The user can check the default value and change each value if necessary or keep the default value. User privacy policy is the list that reflects user's intention determined as above. The user privacy is created by mapping this user privacy policy and the information application schema of each user.

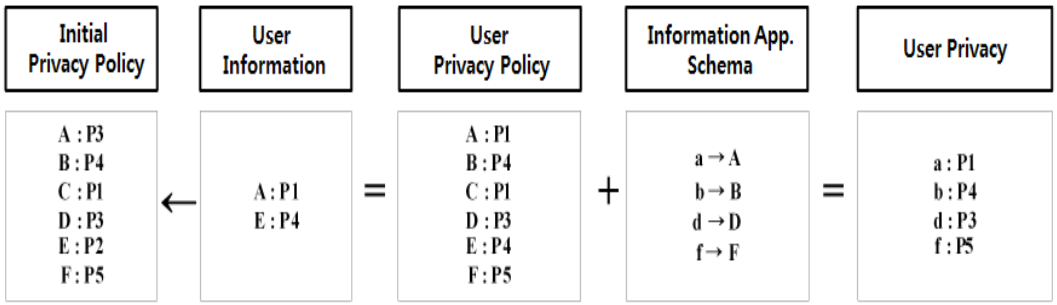


Figure 7. User Privacy Generation Mechanism

The example in Figure 7 shows a process where a user creates his/her privacy policy for the information belonging to a service group. The privacy policy-based protection system allows the user to make decisions by services handling similar information while automatically creating and distributing the user privacy of the user to be given to this information whenever there is user input.

In the example, the user changed the privacy policy for A and E concerning the service group and the user privacy policy of the user is created by reflecting this value. Also, the user privacy relating to the mapping with the user privacy policy and information application server schema is created and transmitted since the information application schema is different.

3.3. Access Group Creation Mechanism

The purpose of the access group is to allow the owner of information to authorize the person he/she selects to access his/her information by designating the mobile phone number of the person to authorize to the designated access authority level. Currently, the privacy policy-based protection system allows the user to set access authority level from 0 ~ 9, and larger number indicates higher access authority for information. When the privacy policy-based protection system receives user input, it creates a security token based on the input, and

currently SHA1 is used as the algorithm for creating a security token. The access group is divided into the user access group which provides the security token created based on user input, the initial access group which provides the token to be used as the default value for each access group when there is no user defined value, and the privacy level which designates the level of the information to be given as default value to those who are not designated by the user.

1 access group of 1 user is given to each service group, and it is newly created and sent to the companies included in each service each time the user defined value changes. For the request for the access to user information, each company controls the access through the mechanism of comparing the security token provided with the request and the security token presented to the access group.

4. Result of Implementation

4.1. Privacy Policy-Based Protection System Implemented

① Request the test page for his/her own (Ye-seul Han) information through PC web ② Request directory server for URL information through the service gateway ③ Access URL address of the information application server at the service gate way through the directory server ④ Connect to information application server and check the information the user wants ⑤ Provide the information appropriate for the privacy level ⑥ A third party requests for the information of Ye-seul Han through the test page using PC web ⑦ Same as ②~⑤.

4.2. Operating Process of Privacy Policy-Based Protection System

Describe the detailed operating process of the smart grid policy-based privacy protection system realized in this study.

1) Requesting for Information using PC or Mobile Device

The user (Ye-seul Han) checks his/her information displayed on the test page and requests for information. Select server and port and check the device code and then display users who wish to access and check the information up to device verification code.

2) Connect to URL through Service Gateway

Requests for URL through user information and connects to the requested URL. The connected URL appears as in Figure 19, and when the user is connected to the available service, a window to check his/her information will appear.

3) Provide the information appropriate for the privacy level (the user himself/herself)

The user's information will appear, and the screen will display the list containing user name, social security number, telephone number, symptom of trouble, diagnosis of trouble, and repair of trouble, details of trouble, and recent wattage through which the user's information can be checked.

4) Provide the information appropriate for the privacy level (others)

The user's information will appear, and the screen will display the list containing user name, social security number, telephone number, symptom of trouble, diagnosis of trouble, and repair of trouble, details of trouble, and recent wattage through. However, if the user is

not Ye-seul Han, the access to information will be blocked with the message, "Privacy is protected."

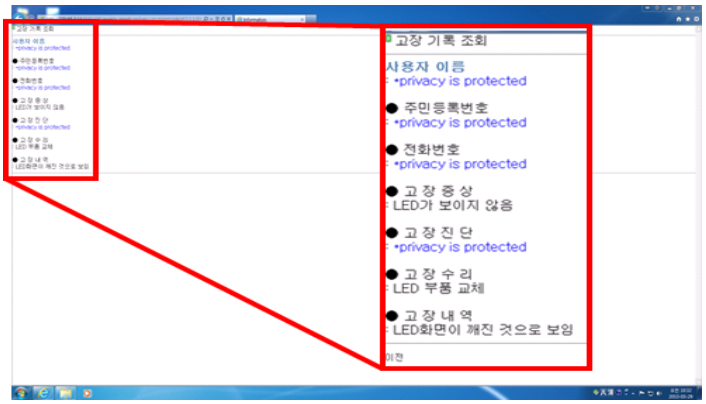


Figure 8. Result of Protected Privacy Information

4.3. Delay Time and Threshold Value Against Frequency of Requests for Secure Sessions

We measured the increase in delay time caused by an increase in the rate of requests for creating security sessions covering the terminal to the network Information Server and the threshold value that allows for session completion. Encryption/decryption of security keys and delays in session creation owing to network transmission and performance of the mobile phone platform were also analyzed for comparison. Various session connections were attempted in a mobile device with network information such as Information Server, and an environment identical to one wherein a link sessions is created using multiple such mobile terminals.

The measured average delay is shown in [Figure 9]. The time taken in creating sessions increase with the request rate, reaching 1000–1500 ms at 40 sessions, 1800 ms at 50, but session errors at 60 sessions. Looking at the status of processing based on the number of requested sessions per second as measured on the server in Figure 10, the processing of up to 50 sessions is entirely possible; but at 60, the processing rate begins to decline. Therefore, the number of security sessions that can be simultaneously processed in the implemented system and on the network IS was estimated to be approximately 60.

In the case of general service session, if the number of sessions requested per second increases up to 120, the time increases up to about 2000–2500 ms, with session delay times dramatically increasing at 120 sessions; session errors occur with 140 requests. Thus, up to 130 simultaneously requested sessions can be processed, but the session processing rate radically declines at 140. Therefore, the number of service sessions that can be simultaneously processed in the test terminal and on the server is estimated to be 140.

A comparison of the results shows that the existence of support for access control and data security increases session delays. Nonetheless, the overhead because of the security function is estimated to be about twofold to conventional overhead. This is believed to be attributable to the problems arising from resource allocation when processing secure service session requests by the handset. By comparison, in the case of the nonsecure service, session processing capability is expected to be high since information processing is carried out on a simple information data.

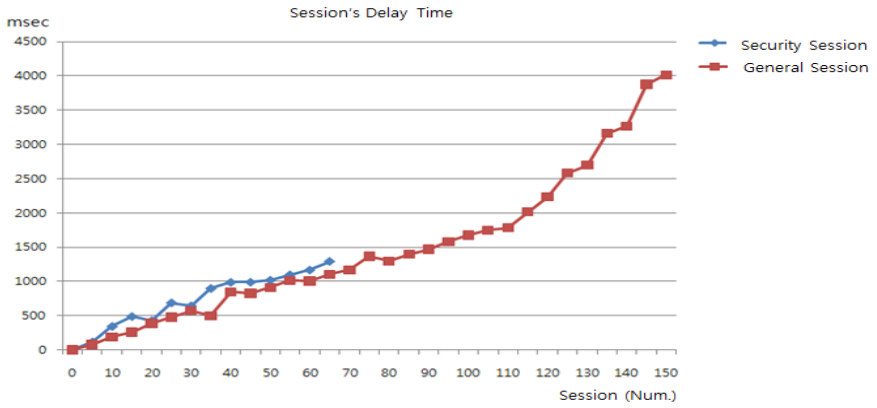


Figure 9. Delay vs Request Rate for Sontinuous Service Sessions

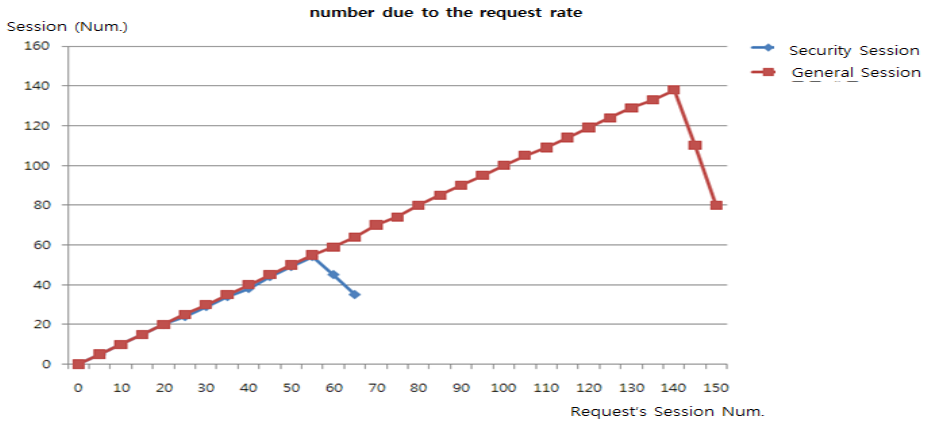


Figure 10. Processing Number Due to the Request Rate for Security

5. Conclusion

The invasion of privacy in the smart grid involves high risk of disclosing personal information from the level of collecting trivial information up to the level of the individual behavioral pattern based on the information collected. For this, the invasion of privacy is becoming the center of interest and a number of studies have been made to resolve this issue. Smart grid minimizes the environmental contamination factors through more efficient use of power and green energy and is the major power network to be used in near future. However, its growth may slow down or it may disappear even before it is fully developed and applied in the midst of anxiety that people may develop if the problem of privacy invasion in the smart grid persists. Under the circumstances, this study developed the privacy policy-based protection system to resolve the issue of privacy invasion.

The privacy policy-based protection system is designed to allow the user to directly set the privacy level of each item and designate the access level for the third party to block the access of undesignated user and protect important information.

Acknowledgements

This work was supported by the Industrial Strategic Technology Development Program funded by the Ministry of Knowledge Economy(MKE, Korea). [10038653, Development of Semantic based Open USN Service Platform]. Corresponding author.(namjepark@jejun u.ac.kr)

References

[1] J. Lee and N. Park, "Individual Information Protection in Smart Grid", T.-h. Kim et al. (Eds.). SecTech/CA/CES-CUBE 2012, CCIS 339, Springer, **(2012)**, pp. 153-159.
[2] N. Park, J. Kwak, S. Kim, D. Won and H. Kim, "WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment", Shen, H.T., Li, J., Li, M., Ni, J., Wang, W. (eds.) APWeb Workshops 2006. LNCS, Springer, Heidelberg, vol. 3842, **(2006)**, pp. 741-748.
[3] N. Park, "Security scheme for managing a large quantity of individual information in RFID environment", Zhu, R., Zhang, Y., Liu, B., Liu, C. (eds.) ICICA 2010. CCIS, Springer, Heidelberg, vol. 106, **(2010)**, pp. 72-79.
[4] N. Park, "Secure UHF/HF Dual-band RFID: Strategic Framework Approaches and Application Solutions", ICCCI 2011. LNCS, Springer, Heidelberg, **(2011)**.
[5] N. Park, "Implementation of Terminal Middleware Platform for Mobile RFID computing", International Journal of Ad Hoc and Ubiquitous Computing, vol. 8, no. 4, **(2011)**, pp. 205-219.
[6] N. Park and Y. Kim, "Harmful Adult Multimedia Contents Filtering Method in Mobile RFID Service Environment", Pan, J.-S., Chen, S.-M., Nguyen, N.T. (eds.) ICCCI 2010. LNCS(LNAI), Springer, Heidelberg, vol. 6422, **(2010)**, pp. 193-202.
[7] N. Park and Y. Song, "AONT Encryption Based Application Data Management in Mobile RFID Environment", Pan, J.-S., Chen, S.-M., Nguyen, N.T. (eds.) ICCCI 2010, LNCS(LNAI), Springer, Heidelberg, vol. 6422, **(2010)**, pp. 142-152.
[8] N. Park, "Customized Healthcare Infrastructure Using Privacy Weight Level Based on Smart Device", Communications in Computer and Information Science, Springer, vol. 206, **(2011)**, pp. 467-474.
[9] N. Park, "Secure Data Access Control Scheme Using Type-Based Re-encryption in Cloud Environment", Studies in Computational Intelligence, Springer, vol. 381, **(2011)**, pp. 319-327.
[10] N. Park and Y. Song, "Secure RFID Application Data Management Using All-Or-Nothing Transform Encryption", Pandurangan, G., Anil Kumar, V.S., Ming, G., Liu, Y., Li, Y. (eds.) WASA 2010. LNCS, Springer, Heidelberg, vol. 6221, **(2010)**, pp. 245-252.
[11] N. Park, "The Implementation of Open Embedded S/W Platform for Secure Mobile RFID Reader", The Journal of Korea Information and Communications Society, vol. 35, no. 5, **(2010)**, pp. 785-793.
[12] Y. Kim and N. Park, "Development and Application of STEAM Teaching Model Based on the Rube Goldberg's Invention", Lecture Notes in Electrical Engineering, Springer, vol. 203, **(2012)**, pp. 693-698.
[13] N. Park, S. Cho, B. Kim, B. Lee and D. Won, "Security Enhancement of User Authentication Scheme Using IVEF in Vessel Traffic Service System", Lecture Notes in Electrical Engineering, Springer, vol. 203, **(2012)**, pp. 699-705.
[14] K. Kim, B. Kim, B. Lee and N. Park, "Design and Implementation of IVEF Protocol Using Wireless Communication on Android Mobile Platform", Communications in Computer and Information Science, Springer, vol. 339, **(2012)**, pp. 94-100.
[15] Y. Ko, J. An and N. Park, "Development of Computer, Math, Art Convergence Education Lesson Plans Based on Smart Grid Technology", Communications in Computer and Information Science, Springer, vol. 339, **(2012)**, pp. 109-114.
[16] Y. Kim and N. Park, "The Effect of STEAM Education on Elementary School Student's Creativity Improvement", Communications in Computer and Information Science, Springer, vol. 339, **(2012)**, pp. 115-121.
[17] V. R. Vinayak, "An Intelligent Neural-Wireless Sensor Network Based Schema for Energy Resources Forecast", IJAST, vol. 34, **(2011)**, pp. 55-64.
[18] R. Sheikhpour, S. Jabbehdari and A. Khadem-Zadeh, "Comparison of Energy Efficient Clustering Protocols in Heterogeneous Wireless Sensor Networks", IJAST, vol. 36, **(2011)**, pp. 27-40.
[19] B. S. Anami and V. B. Pagi, "Multi-stage Acoustic Fault Diagnosis of Motorcycles using Wavelet Packet Energy Distribution and ANN", IJAST, vol. 49, **(2012)**, pp. 47-62.
[20] A. Afzaal Abbasi and A. Kamal, "An Intelligent Neural-Wireless Sensor Network Based Schema for Energy Resources Forecast", IJAST, vol. 33, **(2011)**, pp. 121-130.

