International Journal of Smart Home
Vol.7, No.5 (2013), pp.145-154
http://dx.doi.org/10.14257/ijsh.2013.7.5.15

A Design of Advanced Authentication Method for Protection of Privacy in M2M Environment

Byung Wook Jin[1] and Hyun Hahm[2*]

[1]*Department of Computer Science, Soongsil University*
Seoul, South Korea
[2] *Department of Broadcasting & Digital Media, Chungwoon University,*
Hongseong, Chungnam, South Korea
[1]*quddnr4511@naver.com,* [2]*poparts@chungwoon.ac.kr*

Abstract

M2M (Machine-to-Machine Communication) refers to technologies that allow wired and wireless systems to communicate with other devices with similar capabilities. M2M has special features which consist of low electricity consumption, cheap expenses, WAN, WLAN and others. Therefore, it can communicate via a network. Also, it can handle itself without a person's management. However, it is difficult to manage and control each equipment because of the characteristics of M2M, and it succeeds the weaknesses and security threats of existing wired and wireless networks as it is still used. So In this Paper, It suggests the privacy protection technique planning among Device, Gateway and Network Domain in the M2M environment. The proposal protocol protects a privacy and it also assures a confidentiality and an integrity of the messages when it communicates through Device Domain and Network Domain by using the attribute based cryptography.

Keywords: *M2M, Attribute Encryption, Privacy Security Technique*

1. Introduction

M2M is communication process between machine and machine with no intervention by people or with at least intervention by people, M2M refers to wire and wireless communication between the machines which have similar characteristics. Because of M2M communication, M2M communication devices require to be managed in low electricity, small scale, low cost, WAN, WLAN, and with no management by people [1-2, 10, 11]. M2M system is installed at the remote place which may be lack of basic security and should be used for long time, which is necessary to manage for the functionality. In case of installing M2M in a condition that requires many uses, it is necessary to have many M2M devices, and most of them are mobile devices which are impossible to control and to manage individual device well, which is unrealistic [3, 9, 12, 13].

Therefore, the authentication and message privacy used in M2M devices and system are vulnerable, and it's necessary to have relevant security technology. Based upon this situation of M2M, this study presents a new way to authorize M2M Device and Gateway Domain and to communicate between the authorized devices which make better off communication method for privacy and security.

ISSN: 1975-4094 IJSH

2. Related Work

2.1. M2M (Machine to Machine)

2.1.1. M2M Communication Architecture: ETSI is studying M2M communication architecture and categorizes M2M communication architecture into M2M Device, M2M Device Domain, M2M Gateway Domain, and M2M Network Domain [6].

(1) M2M Device Domain

M2M Device Domain is made of M2M Device and M2M Area Network. M2M Area Network is the network to provide connectivity between M2M Device and M2M Gateway. And the various technologies, i.e., 802.15, Zigbee, bluetooth, PAN(Personal Area Network) or PLC, M-BUS, Wireless M-BUS, KNX, and LAN (Local Area Network) [1][6].

(2) M2M Gateway

M2M Gateway is made of M2M Application and M2M Capabilities. M2M Gateway protect the interaction among M2M devices by using M2M Application and M2M Capabilities and also play as Gateway so that M2M device can access to Network Domain's access network [1][5].

(3) M2M Network Domain

M2M Network Domain is made of Access Network, M2M Core, Transport Network, M2M and Application which are Management Function and Network Management Function. Access Network provides a function to help M2M Device Domain and M2M Core Network can communicate with each other. M2M core is made of Core Network and Service Capabilities and acts as an essential function in M2M communication. M2M application field refers to the interface which collects data from M2M communication, processes them, and provides them, and so on. M2M Management Function and Network Management Function manage the overall M2M communication architecture and network technology [3][4][14].

2.1.2. Requirement for the Authentication Technology of M2M according to environment: To select the authentication technology, which satisfies the requirements specified in M2M communication environment, is realistic [2, 5,15]. The general requirement of the authentication technology can be drawn as follows:

(1) Device Authentication

Communication server in M2M environment should recognize and authorize the data transferred from authorized devices and should transfer the data to them.

(2) Server Authentication

M2M communication device or Gateway should recognize and authorize whether the M2M communication server is authorized or not.

(3) Encoding the data

In case leakage of the data communicated in M2M may harm socially and financially, the communication in M2M environment should be encoded for its security and integrity.

(4) Non-rejection

M2M communication's authentication technology should provide non-rejection method that the user using M2M devices and Gateway cannot reject the data authorized already.

(5) Compatibility with other environment

The authentication technology used in M2M should have compatibility with other domains and devices.

(6) Effectiveness of Authentication

The authentication technology used in M2M should consider the performance of the pre-existing devices and the limitation of them. And the authentication technology should be compact so that it can be used in any kind of devices.

Apart from these general requirements of authentication technology, it's necessary to meet the security requirement according to each environment and security importance. Therefore, when adopting M2M communication technology, it's necessary to draw the security threats which can be predictable and the requirement of authentication technology which can prevent them [1].

2.2. Attribute based Encryption

Attribute-based encryption was invented by Sahai and others in year 2005, and it encodes and decodes based upon the attributes (*i.e.*, belonging, position, and *etc.*) of each object and the architecture to access. This study presents a protocol using the proxy re-encryption based attribute. It extended the pre-existing proxy re-encryption to the attribute-based encryption method and can give users right to re-encrypt in access-control environment. It is featured that users can define freely the proxy, which re-encodes encryption from one access policy to another [7, 10, 11].

2.2.1. KP-ABPRE[8]: Generating key in KP-ABE, KP-ABPRE method has architecture to refer the attribute of receiver and can re-encode the encryption from sender KP-ABE. At this time, in order to re-encode by the other receiver having different architecture to access, sender should print out the re-encoded key $rk_{AS->AS'by}$ which sender can change other access architecture AS' with use of the encoded C from proxy based attribute which can be re-encoded. KP-ABPRE encryption is made of six algorithms.

(1) Setup (1^k): It is an algorithm to describe message space M and encryption space C by using Security Parameter k and System Parameter.

① Attribute U is defined like this U = {1, 2, ... n}.

② Each attribute which is i ∈ U included, select randomly t_i from Z_P in even.

③ Select y in even at Z_P which is random.

④ PK < T1 = g^{t1}, ... , T|U| = $T1 = g^{t_1}, \ldots T_{|U|} = gt \mid U \mid, Y = e(g,g)^{y}$ > MK is defined as <t_1 , … , $t_{|U|}$, y>.

(2) KeyGen(MK, T): It is an algorithm to print out public key PK and security key SK with input of security Parameter 1^k.

① If $T(\gamma)$ = 1, print out key to the user who is able to re-encode.

② Private value $g^{\frac{q_x(0)}{t_i}}$, send i = att(x) to the user.

(3) Encrypt (PK, M, γ): It is an algorithm to print out encryption C_1 throughout the set of attribute γ_1 and the message M.

① Encryption message define $M \in G_2$ in the set of attribute, and select random value $s \in Z_p$.

② Coded message C generated is defined as follows:

$$C = < \gamma, E=MY^r, \{E_i= T_i^S \}_{i \in \gamma} > i$$

(4) RKExtact(γ_1, γ_2) : it is an algorithm to print out the unilaterally re-encoded key $rk_{1->2}$ which is the private key and the set of γ_2

① re-encoded key is $RK_1^{A->B} = t'_1/t_1$, $RK_1^{A->B} = t'_2/t_2$, … , $RK_{|\gamma|}^{A->B} = t'_{|\psi|} / t_{|\psi'|}$

(5) Re-encryption: it is an algorithm to print out C2 which is re-encoded or "rejection" by inputting the re-encoded key $rk_{1->2}$ and cryptogram C1.

① γ_2 is the set of the attribute of receiver and $s \in Z_p$.

②C_2 is a cryptogram which is re-encoded and defined as follows:

$$C_2 = (\gamma', E'=MY^{rs}, \{E_i=((T_i^r)^{RK_i^{A->B}})^s\}_{i \in \gamma}$$

(6) Decrypt (E, D, x): it is an algorithm to print out the plain text corresponding to the cryptogram by inputting the private key and a cryptogram C_2, (in case of no corresponding with, printing out $\perp$).

① The first level cryptogram C_{ψ_1} is given and the re-encoded key $RK_1^{A->B}$ is given.

$$C_{\psi_1} = (\gamma_1, E'=MY^r, \{E_i= T_i^r \}_{i \in \gamma})$$

$$RK_1^{A->B} = t'_1/t_1, RK_1^{A->B} = t'_2/t_2, \ldots , RK_{|\gamma|}^{A->B} = t'_{|\psi|} / t_{|\psi'|}$$

② The second level cryptogram can be acquired with the first level cryptogram and the re-encoded cryptogram which are given to.

$$C_{\psi_2} = (\gamma', E'=MY^{rs}, \{E_i=((T_i^r)^{RK_i^{A->B}})^s\}_{i \in \gamma}) = (\gamma', E'=MY^{rs}, \{E_i=((T_i^{rs})\})$$

③If node x = LeafNode, DecryptNode(E, D, x) = $e(D_x, E_i)$ $e(, g^{\frac{q_x(0)}{t_i}} g^{s \cdot t_i}) = e(g, g)^{s \cdot qx(0)}$, if $i \in \gamma$, then $\perp$

④ If $F_z \neq \perp$, then $F_x = \prod_{z \in S_x} F_z^{\Delta i, S'_x(0)}$, $S'_x = index(z) : z \in S_x$

$$= \prod_{z \in S_x} e(g,g)^{r \cdot q_z(0)})^{\Delta i, S'_{x(0)}}$$

$$= \prod_{z \in S_x} e(g,g)^{r \cdot q_{parent}(z)^{index(z))}})^{\Delta i, S'_{x(0)}}$$

$$= \prod_{z \in S_x} e(g,g)^{r \cdot q_x(i) \cdot i, \Delta S'_{x(0)}})$$

$$= e(g, g)^{s \cdot q_x(0)}$$

3. Proposed Communication Technique

3.1. Whole Architecture

The configuration chart of authentication and message privacy protection system, which is based on attribute encryption method proposed in M2M, is shown in the Figure 1 below.

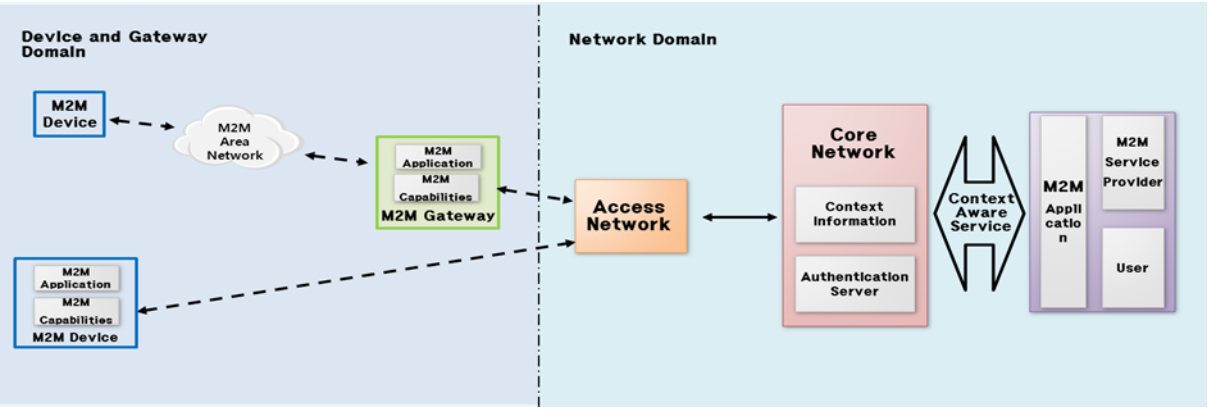

Figure 1. Configuration of the Entire System is also Proposed

It shows that setups and key can be generated in Access Network, based upon attribute encryption technique. System authorizes M2M Device and Gateway with use of the generated key and is designed to protect the privacy between the authorized device and Network Domain.

The protocol, which was suggested, should satisfy the requirement as follows:

(1) The devices in Device and Gateway Domain Devices should know the parameter of Access Network's Server.

(2) The serial number of the device, which receives and sends the authentication information and message, should be registered in advance, in Access Network of Network Domain.

3.2. Setup and Key Generating

Setup and key are generated in Access Network of Network Domain in order to receive and send the authentication data and message of device and Gateway in M2M Device and Gateway Domain. Setup and key generating based upon attribute encryption technique is as follows:

① System Parameter is defined with use of Access Network Setup (1^k) algorithm and, the public key pk and the master key mk are generated.

② Access Network's private value D_x is generated with use of KeyGen(mk, T) algorithm.

3.3. Authentication Protocol

Device authentication protocol is suggested with use of the key generated in Network Domain's Access Network. Authentication protocol is shown in the following Figure 2. Device requests Server to authenticate between device and Access Network's Server.

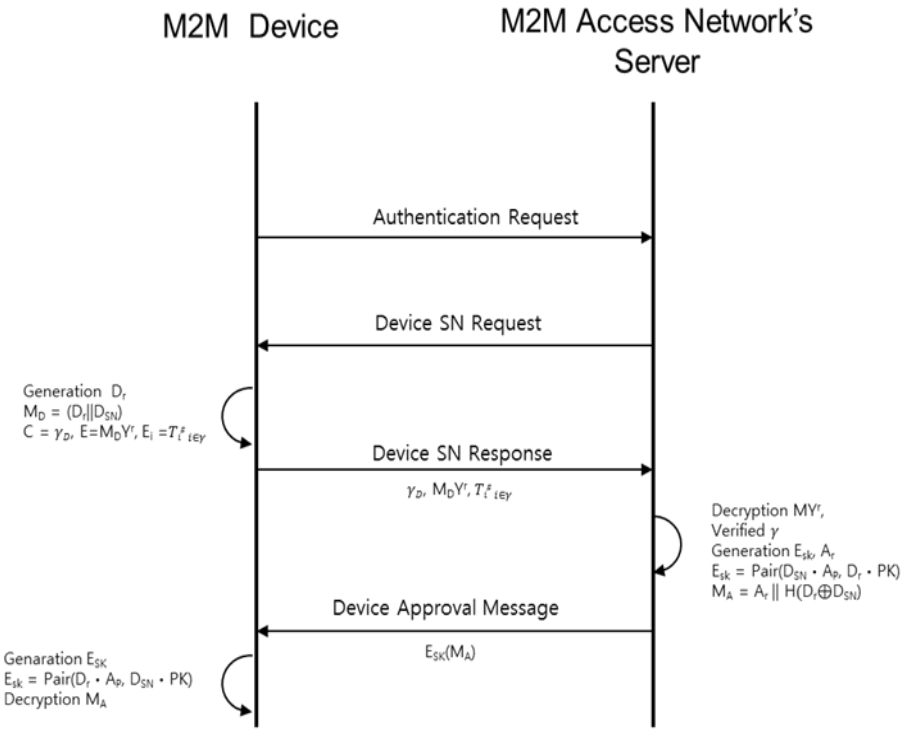

Figure 2. Device Authentication Protocol

① Server requests Device's SN, and after device generated D_r, M_D is generated in connection with Device's D_{SN} and D_r.

② Device sends cryptogram $C = \langle \gamma, M_D Y_r, \{E_i = T_i^S\}_{i \in \gamma} \rangle$ to Server

③ Server encodes the cryptogram given to, validates γ, generates E_{SK}=Pair(D_{sn}•A_P, D_r•PK) with identity based system, generates message M_A = Ar || H($D_r \oplus D_{sn}$), encodes it as E_{Sk}, and finally sends it to Device.

④ Device generates E_{sk} = Pair(D_r •A_P, D_{sn} •PK) and then encodes M_A with identity-based system.

3.4. Message Passing System

Message passing system ensures that message privacy between the device authenticated and Network Domain Server' application should be secure, and the process is shown in the following Figure 3.

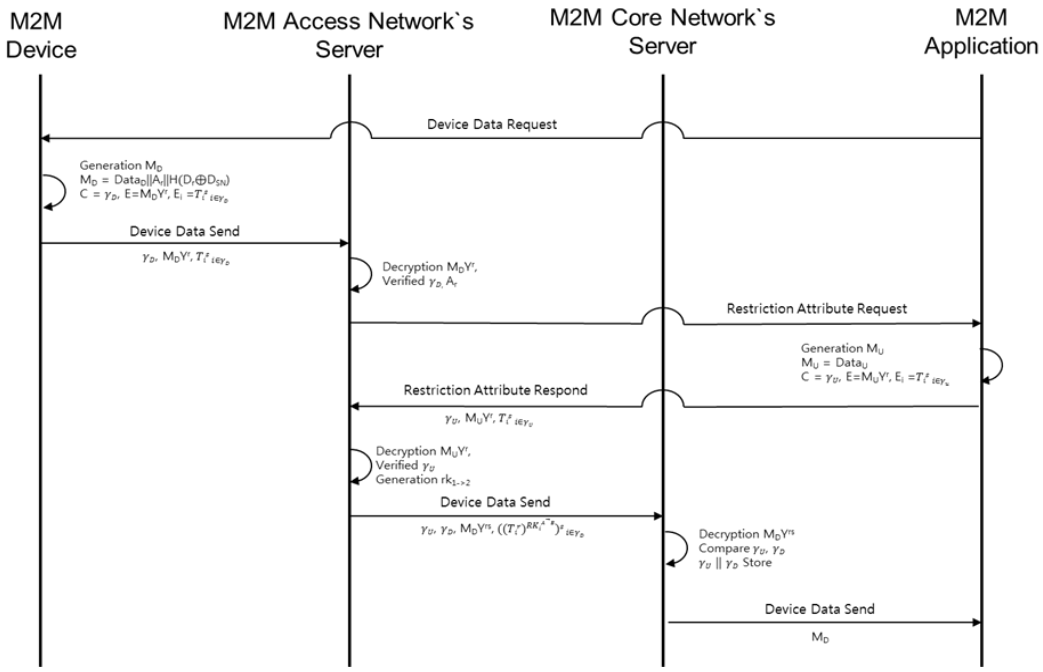

Figure 3. Detailed Protocol of the Proposed System

① User or service provider requests Device to send Data through Application.

② After Device generated M_D = ($Data_r$ || A_r || $H(D_r \oplus D_{sn})$, Device encodes it and sends C = < γ_D, $M_D Y^r$, $\{E_i = T_i^S\}_{i \in \gamma_D}$ > to Access Network's Server.

③ Access Network's Server re-encodes the cryptogram received, validates γ_D and A_r, and then requests Application to allow access right.

④ Application generates M_U=$Data_U$, encodes Application attribute and the data, sends C = < γ_U, $M_D Y^r$, $\{E_i = T_i^S\}_{i \in \gamma_U}$ > to Access Network's Server.

⑤ Access Network`s Server re-encodes the cryptogram received, validates γ_U, and generates $_{rk1->2}$ by using RKExtract(γ_U , γ_U) algorithm.

⑥ Access Network's Server send < γ_U , γ_D , $M_D Y^{rs}$, $\{E_i = T_i^S\}_{i \in \gamma_U}$ > to Core Network`s Server by using re-encryption algorithm with $rk^{1->2}$.

⑦ Core Network`s Server re-encodes the cryptogram received, compares γ_U with γ_D and validates them, saves them, and then sends M_D to Application.

4. Safety Analysis

At this chapter, this study analyses the security of message privacy communication which uses attribute-based encryption. The communication method presented should ensure that the security system can protect the message integrity and the confidentiality and Core Network has M2M's specific characteristics from disguise attack and man in the middle attack. Safety is explained as follows:

(1) Security risk of Device Message Confidentiality and Privacy

It is possible that the data can be exposed to attacks, such as bugging, Sniffing, and Spoofing while M2M Device or Gateway is sending message to Network Domain, and the confidentiality of data gets in trouble. The communication presented by this study can send and receive data safely by the use of attribute-based encryption method and can provide the safety for privacy by the use of attribute Parameter, which helps to prevent the unidentified access from occurring.

(2) Disguise Attack

One of typical disguise attack against M2M environment is an attack, which disguises Device or Server. To prevent this kind of attack, it should be ensured that message encoded through E_{SK} generated with identity based system will be sent and received. Also, comparing and analyzing the attribute and then saving it can help to communicate more safely.

(3) Man in the Middle Attack

The communication method presented by this study can provide better off safety from man-in-the-middle-attack by using the session key generated identity based system and by comparing and analyzing the data from Device with attribute-based encryption.

(4) Attack against Core Network

The attacks against Network Domain's Core Network are targeting for the security vulnerability of Core Network, such as service denial attack, disguise attack, moving to unauthenticated place, and *etc*. The communication method presented by this study can provide safety for Core Network from the attacks by validating serial number of device and Gateway in Network Domain and by using attribute-based encryption technique in M2M environment.

5. Conclusion

This study presented a communication method which can increase safety and can complement the vulnerability of M2M environment and also presents a communication way which can protect message privacy and Device and Gateway Domain's authentication by the use of identity-based system between M2M Device and Access Network's Server and by the use of attribute-based encryption technique.

And validating Device, the communication method of this study presented a protocol which can protect the access right to Device and the message privacy with use of the parameter of attribute-based encryption technique, and analyzed the vulnerability of

pre-existing M2M environment, *i.e.*, message integrity and confidentiality, disguise attack, man-in-the-middle-attack, attack against Core Network due to M2M's specific environment. Later on, I think, it's necessary to discuss a communication method which can be used widely with high level security system. And it will be necessary to discuss the effectiveness through the realization of attribute-based encryption technique and the various applications with use of attribute-based encryption technique.

References

[1] G. S. Lee, D. G. Min and M. S. Jun, "A Study on Authentication of Mobile Agency AP Connection Using Trusted Third Party in Smart Phone Environment", Journal of the Korea Academia-Industrial cooperation Society, http://dx.doi.org/10.5762/KAIS.2012.13.11.5496, vol. 13, no. 11, **(2012)**.
[2] K. S. Kim, J. I. NamGoong, J. I. Jung and Y. J. Kim, "M2M Security threats and requirements of service", Telecommunication Technology Association, .TTA, **(2012)**.
[3] I. Cha, Y. Shah and A. U. Schmidt, "Trust in M2M communication", IEEE Vehicular Technology Magazine, **(2009)**.
[4] K. W. Lee and H. I. Jun, "Mechanism of Multimedia Synchronization using Delay Jitter Time", Journal of the Korea Academia-Industrial cooperation Society, http://dx.doi.org/10.5762/KAIS.2012.13.11.5512, vol. 13, no. 11, **(2012)**.
[5] S. Y. Min and S. J. Jang, "A Study on the Protection of Personal Information using a Virtual IDs in an Anonymous Bulletin Board", Journal of the Korea Academia-Industrial cooperation Society, http://dx.doi.org/10.5762/KAIS.2012.13.9.4214, vol. 13, no. 9, **(2012)**.
[6] Y. S. Bae, "A Study of Effect of In Information Security Management System Certification on Organization Performance", Journal of the Korea Academia-Industrial cooperation Society, http://dx.doi.org/10.5762/KAIS.2012.13.9.4224, vol. 13, no. 9, **(2012)**.
[7] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-based Encryption for fine-grained access control of encrypted data", Proceeding Of ACM CCS'06, Virginia, USA, **(2006)** October 89-98.
[8] G. Shanqing, Z. Yingpei, W. Juan and X. Qiulian, "Attribute-Based Re-Encryption Scheme in the Standard Model", Wuhan University Journal of Natural Sciences, China, Hubei, vol. 13, no. 5, **(2008)**, pp. 621-625.
[9] G. Zhang and Q. Xu, "Secret Key Awareness Security Public Key Encryption Scheme", International Journal of Security and Its Applications, vol. 5, no. 5, **(2011)**.
[10] W. Yau, R. C. W. Phan, S. H. Heng and B. M. Goi, "Proxy Re-encryption with Keyword Search: New Definitions and Algorithms with Proofs", International Journal of Security and Its Applications, vol. 5, no. 2, **(2011)**.
[11] J. P. Arnau, D. R. Monedero and J. Forne, "A Privacy-Protecting Architecture for Recommendation Systems via the Suppression of Ratings", International Journal of Security and Its Applications, vol. 6, no. 2, **(2012)**.
[12] J. Zhang, Y. Cui and Z. Chen, "SPA: Self-certified PKC-based Privacy-preserving Authentication Protocol for Vehicular Ad Hoc Networks", International Journal of Security and Its Applications, vol. 6, no. 2, **(2012)**.
[13] W. Go and J. Kwak, "Privacy-Enhanced Secure Data Transaction System for Smart Grid", International Journal of Security and Its Applications, vol. 6, no. 3, **(2012)**.
[14] M. Yoon, Y. K. Kim and J. W. Chang, "A New Data Aggregation Scheme to Support Energy Efficiency and Privacy Preservation for Wireless Sensor Networks", International Journal of Security and Its Applications, vol. 7, no. 1, **(2013)**.
[15] J. Qiuyan, K. W. Lee and D. H. Won, "Study on A Secure Remote User Authentication Scheme Using Smart Cards", International Journal of Security and Its Applications, vol. 7, no. 2, **(2013)**.

Authors

Byung Wook Jin received his B.S. degree in Multimedia Science from ChungWoon University, Chungnam, Korea, in 2011, and M.S. degree in Computer Science from Soongsil University, Seoul, Korea, in 2013. He is currently a Ph.D Course in the Computer Science, Soongsil University. His research interests include Machine to Machine, Authentication System, Network Security.

Hyun Hahm received his B.F.A. degree in Radio & TV Broadcasting, Film from California State University Los Angeles, USA in 1997, and his M.A. degree in Broadcasting from Chung-Ang University, Seoul, Korea in 2001. Ph.D. degrees in Visual Culture course finished from Korea University, Seoul, Korea in 2010. From 1992 to 2001, he worked as a producer in broadcasting network system. He is now an Associate Professor in the Department of Broadcasting & Digital Media, Chungwoon University, Hongsung, Korea. His research interests include broadcasting, visual communication, and visual cultures.