International Journal of Security and Its Applications
Vol. 10, No. 12 (2016), pp.43-52
http://dx.doi.org/10.14257/ijsia.2016.10.12.05

Meter-HES Mutual Authentication in the Smart Grid AMI Environment

Seung-hwan Ju[1], Young-in Park[1], Sang-gyoo Sim[1], Myung-chul Lim[1], Sung-hyu Han[2] and Hee-suk Seo[3*]

[1]*Penta IoT Convergence Lab. Pentasecurity System Inc, South Korea*
[2]*School of Liberal Arts & HRD, KoreaTech, South Korea*
[3]*Department of Computer Science and Engineering, KoreaTech, South Korea*

Abstract

AMI (Advanced Metering Infrastructure) is one of the ways to build a smart grid environment, this is the automated power metering. We design the mutual authentication on the AMI environment verify the both sides, and provide a secure communication channel. This paper is a study of AMI Security in Penta Security System, which is provided in real AMI deployment environment. We have used the technique such as PKI with DTLS, certificates for implementing secure AMI. The study will be used for equipment validation study in IoT environment.

Keywords: *AMI, Authentication, IoT, SmartGrid, Security, PKI*

1. Introduction

Energy grid control system is separate from the public network, but it is Power systems are becoming more comprehensive and stringent security guidelines required while increasingly relying on IP (Internet Protocol) based systems in smart grid deployments. The smart grid is a generic term efficiency, reliability and above the next-generation power grid to increase the stability of the grid. It uses the following technique for this purpose;

Intelligent devices, two-way communications, advanced control systems, intelligent storage system.

Smart Grid system was applied to the AMI (Advanced Metering Infrastructure) system for efficient management in the grid. This control system has also the same as the vulnerability information that is the target of attack in an information communication network, because information is generated and stored through the public communication network. Thus, AMI of the smart grid must be able to protect the user's privacy, and data encryption.

A public key infrastructure (PKI) supports the distribution and identification of public encryption keys, enabling users and computers to both securely exchange data over networks such as the Internet and verify the identity of the other party.

Without PKI, sensitive information can still be encrypted (ensuring confidentiality) and exchanged, but there would be no assurance of the identity (authentication) of the other party. Any form of sensitive data exchanged over the Internet is reliant on PKI for security.

A typical PKI consists of hardware, software, policies and standards to manage the creation, administration, distribution and revocation of keys and digital certificates. Digital certificates are at the heart of PKI as they affirm the identity of the certificate subject and bind that identity to the public key contained in the certificate.

* Corresponding Author

ISSN: 1738-9976 IJSIA

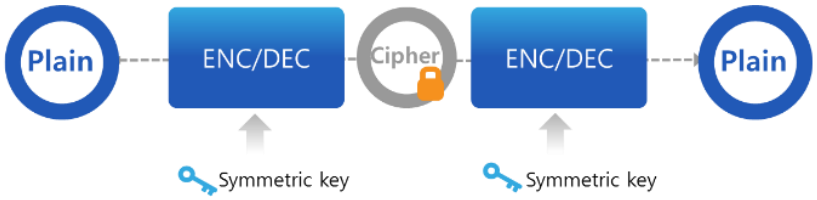

Figure 1. 3D Symmetric Key Encryption

This security is vulnerable when one of the two keys are exposed. We need a KMS (Key Management System) to overcome this problem. Symmetric key encryption technology is less constrained performance requirements, characterized in that the speed is fast, it is suitable for high-volume data encryption.

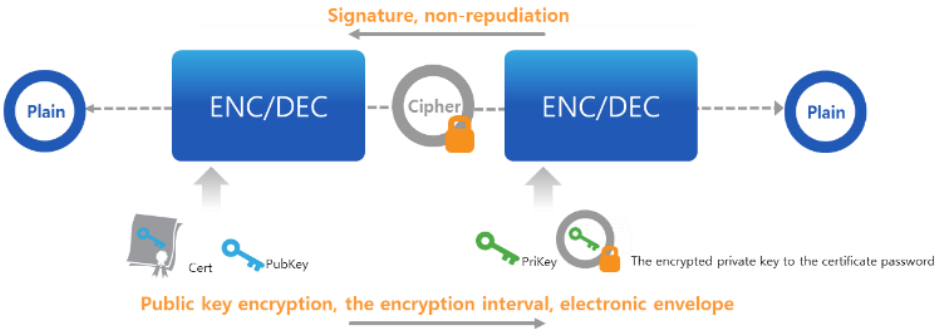

Figure. 2. Public Key Encryption

In this study, we tried to establish a secure communication channel to perform mutual authentication between meter nodes and server.

2. The Threat of the AMI Environment

2.1. Attacks on Meter Nodes

An attacker with access to a physical smart meters, it is possible to extract important information to decompose the meter hardware. If someone make malware on the basis of the knowledge of the secure smart meters, this can modify the measurement information and attack to the control system. Meter nodes infected with malicious code can spread malicious code themselves to infect surrounding smart meters. Smart meters are infected with malware, it will receive the command of the attack, such as denial of service attacks and unauthorized operation.

2.2. Attacks on DCU

If someone is possible physical access of DCU (Data Collecting Unit), who can obtain information through the decomposition device is illegal. An attacker may obtain stored information such as a user ID, a password, an encryption key, the source code and binary of the embedded operating system and the application through the DCU memory dump.

If you can access the network through the DCU, an attacker can obtain administrator permissions of the DCU to find the username and password using a brute-force attacks, and improper account administration vulnerabilities. Once DCU is used for the attack, there is a possibility to be exploited attack vectors that can be accessed on the host system in MDMS (Meter Data Management System) system.

2.3. Attacks on MDMS

If the attacker penetrated the MDMS system, it is possible for a malicious control of the DCU and smart meters. However, it is difficult to direct penetration MDMS system because it is connected to a dedicated network.

So, it involves indirect penetration through the vulnerability analysis of the operating system and applications used by the MDMS, the administrator must check the vulnerabilities, as shown below:

- Operating systems, Web services, and apps (App) services, DB (Database) vulnerability
- Administrator permissions management
- Preparing for storage media such as USB that contains malicious code

3. Mutual Authentication

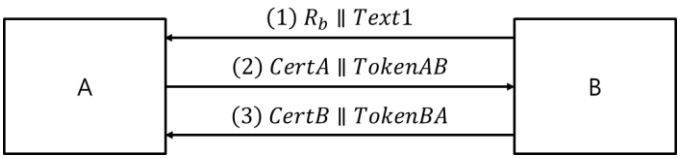

Figure. 3. Mutual Authentication

$$TokenAB = R_A \parallel R_B \parallel B \parallel Text3 \parallel_s S_A(R_A \parallel R_B \parallel B \parallel Text2)$$
$$TokenBA = R_B \parallel R_A \parallel A \parallel Text5 \parallel_s S_B(R_B \parallel R_A \parallel A \parallel Text4)$$

We use the three pass mutual authentication technique for AMI mutual authentication. This is a technique to each other the objects are confirmed (mutual authentication) using the three messages. This technology uses a Random Number Controlled by generating and checking in order to meet the Uniqueness and Timeliness.

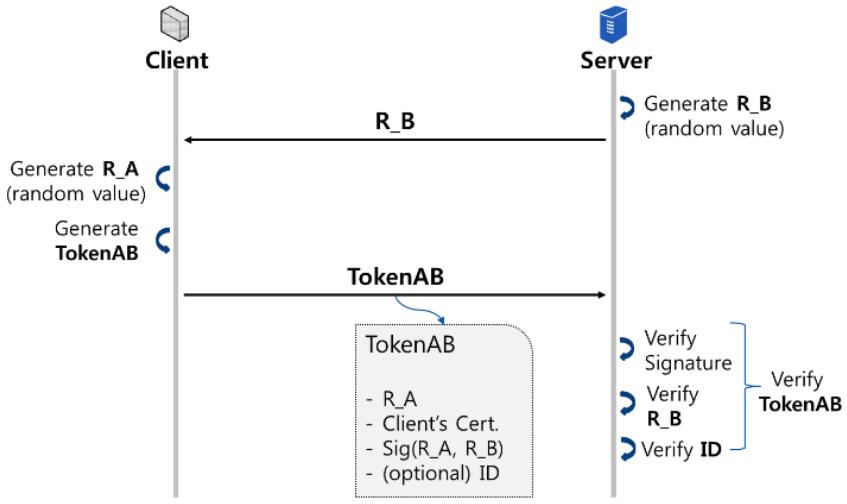

Figure 4. Unilateral Mode

This mechanism only provides authentication using X.509 certificates [7]. It has no effect on the protocol encodings and does not provide integrity or confidentiality services.

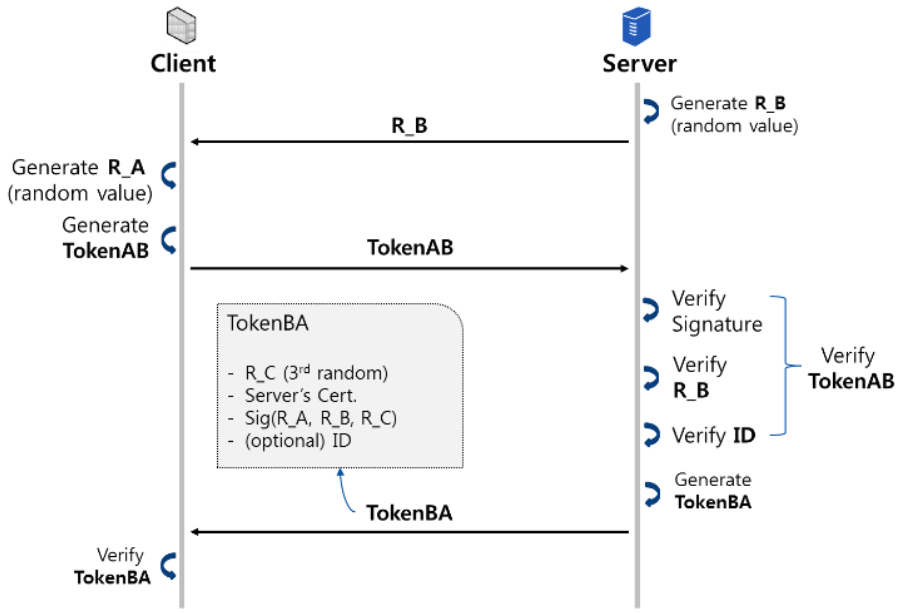

Figure 5. Mutual Authentication Mode

We design the Authentication SASL (Simple Authentication and Security Layer) Mechanism. We have designed Authentication Modes Unilateral and Mutual authentication.

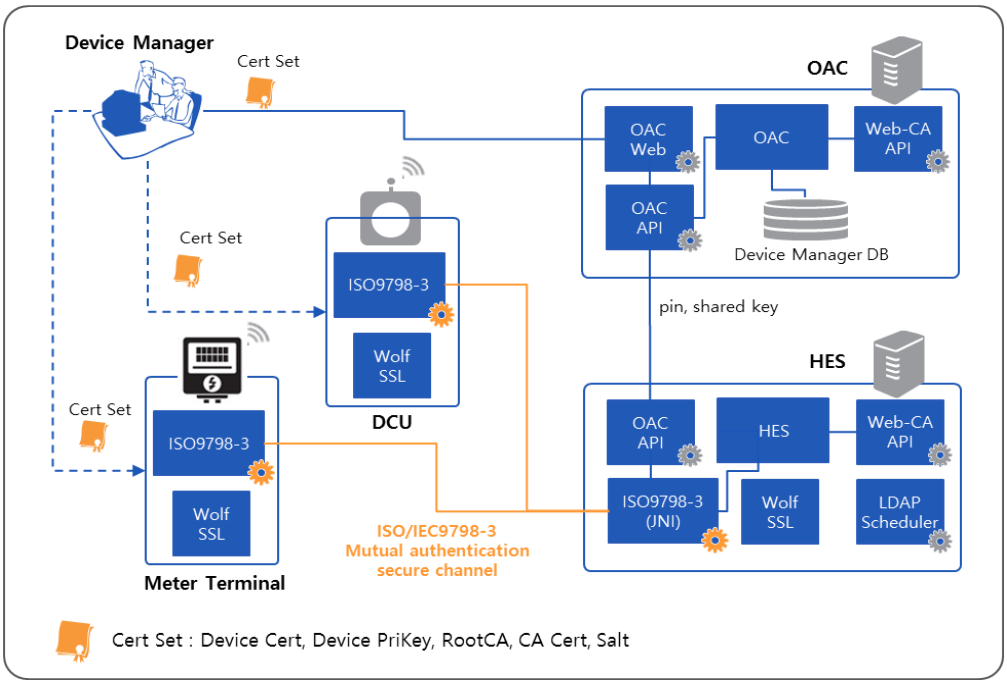

Figure 6. Structure of AMI Authentication System

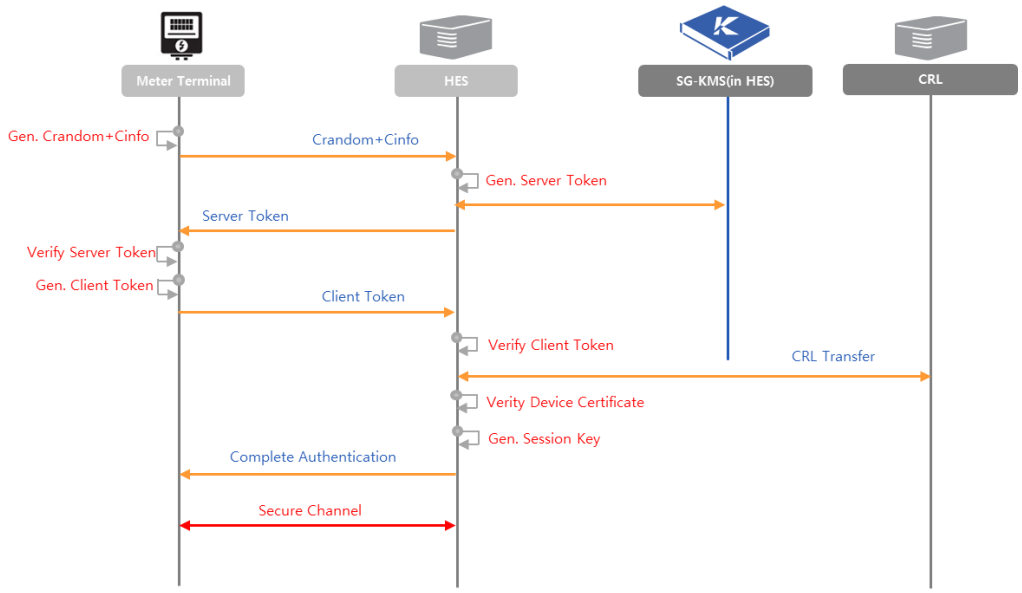

Figure 7. ISO 9798 based Authentication System

4. AMI Authentication System

All AMI communications must be protected from cyberattacks such as unauthorized wiretapping and tampering as well as being guaranteed end-to-end security. As such, the AMI system must provide security services that ensure confidentiality, data integrity, authentication, access control, availability, non-repudiation and key management.

First, the confidentiality of data transferred over the network and data stored in the system and devices in the AMI must be assured. Second, the integrity of data transferred over the network and data stored in the system and devices in the AMI must be assured. Third, mutual authentication between communicating objects must be assured during network communication in the AMI. For that, the smart meter interfacing the utility domain, smart utility network domain and user domain of the AMI, as well as the utility interface system, must be certified by a certification center. Fourth, the AMI must perform access control, which assigns only the minimum privilege to an authorized member when a member of the AMI attempts to access another system or device of the AMI. Fifth, the availability of all networks and services must be assured. Sixth, the non-repudiation service must be provided when billing and demand response data are interfaced over the AMI. Seventh, the encryption key used for AMI information protection must be generated, distributed, stored and disposed of in accordance with safe and legal procedures. The encryption key and certificate owned by each member must be safely managed by the relevant security policy. [9]

We design the Authentication SASL (Simple Authentication and Security Layer) Our AMI authentication system is divided into three parts. One is the meter and DCU (Data Collect Unit) to collect and transmit the measurement information from the client side.

Another one is the server side of the HES to analyze the received transmission data.

The other is the OAC (Online Authentication Center) to manage certificates to be reliable communications on both sides.

4.1. Client Side

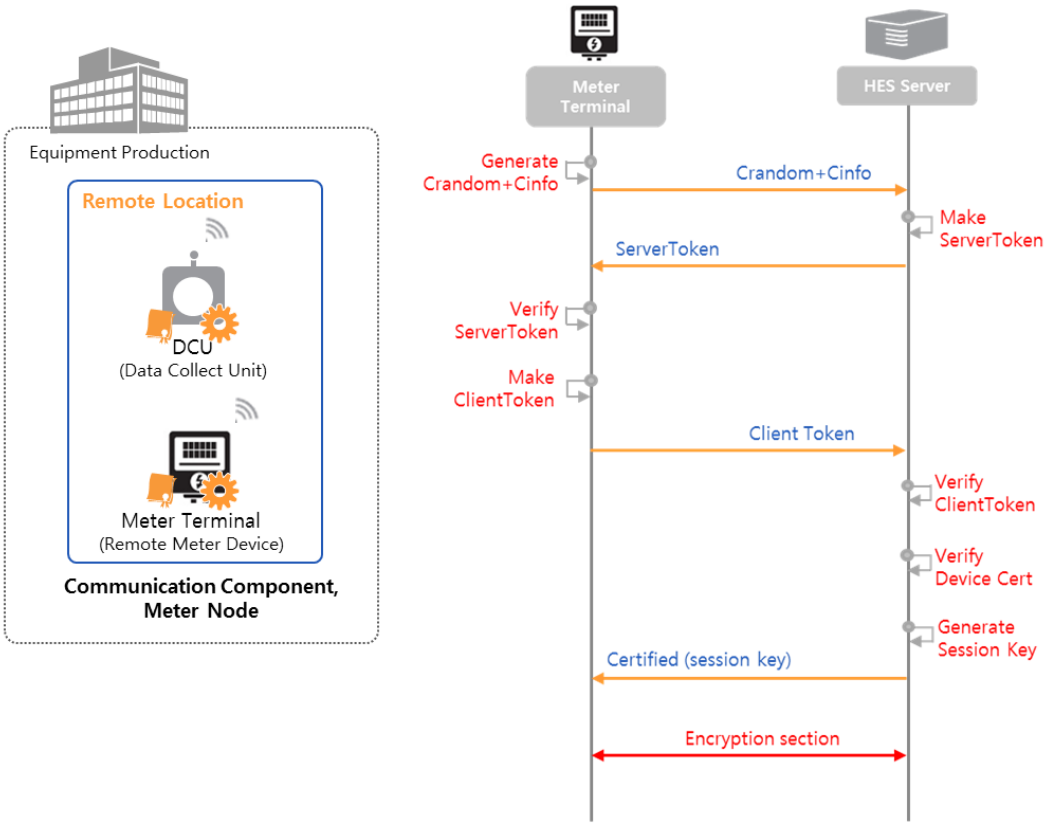

Figure 8. Overview of Client Side (DCU and Meter Terminal) and Authentication Sequence between Meter Terminal and HES

There are DCU and Meter Terminal on the client side.

DCU performs two roles;

1. Data Collector: DCU collects the information of the Meter Terminal.
2. Data Repeater: DCU sends the information to transmit Meter Terminal Server HES

If you use the normal channels of information there is a risk of exposure Meter Terminal. Therefore, it requires a secure channel between Meter Terminal and HES.

So the device and the server mutually authenticate and they establish a secure communications channel.

There are DCU and Meter Terminal on the client side. So it requires authentication process between the server and the HES-meter terminal as shown above.

1. Client sends the random number with the client device to the server.
2. Server generates a token server, using the received information and the server information, and passes it to the client.
3. The client and the server verifies the token, by using the inside information and generates a client token. And it delivers it to the server.
4. Server determines the client to verify the suitability client token, and finally passing the session key to be used for the communication.

4.2. HES

HES is a server that receives transfer data from the DCU.

- Server has a DTSL communication module for fast communication after the mutual authentication.

TLS is a security protocol for enabling applying the TLS UDP (Tansport Layer Security) protocol that provides the security of the Transport layer protocol in TCP and UDP. UDP-based applications can prevent the attacks that can occur on the tapping, interference, such as a network message by using a modulation DTLS.

- The server has the light weight encryption algorithms for mutual authentication.

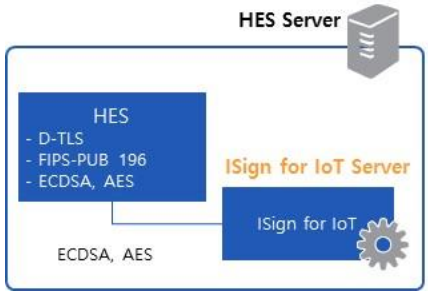

Figure 9. Overview of HES

4.3. OAC

OAC is an online certification center, usually points to the product name. OAC provides the infrastructure for mutual authentication. This consists of a OCA server, WAS, DB and the like.

OAC performs a variety of certificate management tasks, such as registering the objects over the Web, and issuing application, issuance approval, issuance, re-issuance, revocation for the certificates.

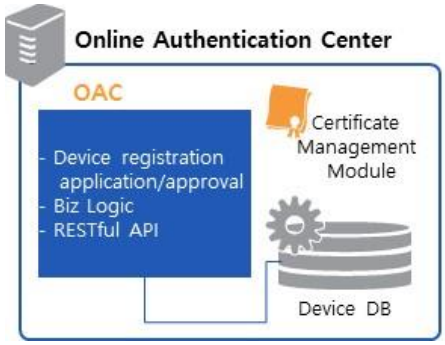

Figure 10. Overview of OAC

5. AMI Mutual Authentication Scheme

The client device is a security module and Meter Terminal on the left in the picture above. Other items are in charge of the server area. We expressed widely communication with the security module and the device server through the HSE above figure.

5.1. Client Side

1. The client creates a token init to their information and transmits it to the server.

A. Security modules obtain the device information from the terminal to the meter, and generates a Crandom available for token generation.

2. The server checks the client information of the client to open the token init.
   A. Server extracts the c_info value from the device information init token to load the Pin argument in the device registered in the device DB.
   B. In the process, the server can determine whether the devices registered with the serial number of the device.
3. The server generates the Server_token to combinate of their own information and information of the client Pin.
   A. In this process, the server generates a Srand available for token generation.
   B. Server delivers as a certificate and the digital signature to verify their suitability to the client.

$$Sign(Srandom+Crandom+Sifno+Pin)$$

4. The client determines the compliance server through the verification of the certificate chain.
   A. The client loads the CA certificate from the CA cert buffer for certificate verification.
   B. And it is determined that the server certificate is a certificate issued from a CA.
   C. Clients combining plain part using the Crandom.

$$Srandom+Crandom+Sinfo+Pin$$

   D. The client confirms the server_token to sign the plaintext to the server certificate. This is the verification procedures of Server_Token.
5. The client generates a client token in the same way as above. And server will validate the client_token in the same way.
6. If the client token verification is completed, the server determines that it has succeeded in forming a secure channel. And it shall issue a session key to be used over a secure channel.

5.2. Communication Key of the Secure Channel

1. Clients need to create a shared key to be used in security communication using the session key received from the server.
   A. The client encrypts the session key Cinfo the value passed to the server.
2. The server deliver the package to the shared key to be used for communication.
   A. Servers that share the same session key may be extracted cinfo decodes the message.
   B. The server loads the encrypted shared key and pin in the DB through cinfo.

$$Enc_{SessionKey}(Enc_{DevicePub}(Shared\ Key) + Pin)$$

3. The client may finally obtained through the twice decoding process of the Shared Key.

   A. $Enc_{SessionKey}(Enc_{DevicePub}(Shared\ Key) + Pin)$

   B. $Enc_{DevicePub}(Shared\ Key)$

   C. SharedKey

After this ends the mutual authentication and key sharing communication, the client and the server is able to communicate a symmetric key shared key.

6. Conclusion

We studied about the PKI technology was to apply it in IoT environment. We studied the security device authentication methods built and implemented an authentication method from the AMI environment. This paper is a study of AMI Security in Penta Security System, which is provided in real AMI deployment environment. We have used techniques such as PKI with DTLS, certificates for implementing secure AMI.

Acknowledgments

Following are results of a study on the "Leades INdustry-university Cooperation" Project, supported by the Ministry of Education, Science & Technology (MEST).

References

[1] S. Lee, “A security mechanism of smart grid AMI network through smart device mutual authentication”, The International Conference on Information Networking 2014 (ICOIN2014). IEEE, **(2014)**.
[2] Y.-A. Jung, “Mutual Authentication Scheme between All AMI Entities in Smart Grid Environment”, International Journal of Multimedia and Ubiquitous Engineering, vol. 11, no. 3, **(2016)**, pp. 411-424.
[3] H. Nicanfar, “Efficient authentication and key management mechanisms for smart grid communications”, IEEE systems journal, vol. 8, no. 2, **(2014)**, pp. 629-640.
[4] Z. Fan, “Smart grid communications: Overview of research challenges, solutions, and standardization activities”, IEEE Communications Surveys & Tutorials, vol. 15, no. 1, **(2013)**, pp. 21-38.
[5] J. Wang and V. CM Leung, “A survey of technical requirements and consumer application standards for IP-based smart grid AMI network”, The International Conference on Information Networking 2011 (ICOIN2011). IEEE, **(2011)**.
[6] H. Nicanfar, P. Jokar and V. CM Leung, “Smart grid authentication and key management for unicast and multicast communications”, Innovative Smart Grid Technologies Asia (ISGT), 2011 IEEE PES. IEEE, **(2011)**.
[7] R. Housley, “Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile”, No. RFC 3280, **(2002)**.
[8] H. Gharavi and B. Hu, “Multigate communication network for smart grid”, Proceedings of the IEEE 99.6 **(2011)**: 1028-1045.

Authors

Seung-hwan Ju, Assistant Manager
- Penta IoT Convergence Lab at PentasecuritySystem. Inc.,
- PhD Candidate at Department of Computer Engineering, Korea University of Technology and Education, Korea
- BS, MS degree from Korea University of Technology and Education, Korea
- Interest: SmartCar Security, Mobile Security, IoT Security

Sung-hyu Han, Associate Professor
- School of Liberal Arts and HRD, Korea University of Technology and Education, Korea
- BS, MS, PhD degree from Yonsei University, Korea
- Interest: Coding Theory, Cryptography, Machine Learning

Hee-suk Seo, Professor.
- Department of Computer Engneering, Korea University of Technology and Education, Korea
- BS, MS, PhD degree from Sungkyunkwan University, Korea
- Interest : Network Security Technology, Security Simulation

