공장 자동화를 위한 RFID 경량 암호 프로토콜에 관한 연구

황 득 영*, 김 진 묵**

요 약

국내에서 공장자동화에 대한 관심이 증가하고 있으며, 이에 관한 개발이 활발하게 시도되고 있다. 특히, '제조업 혁신 3.0 전략'에 따라 중소기업의 제조 공장들에 대한 스마트화에 대한 관심이 급격히 증가하고 있다. 뿐만 아니라, 스마트 공장을 구축하기 위한 정책적, 기술적, 전략적 접근 방법을 모색하고 있다. 하지만 이와 같은 스마트 공장 또는 공장 자동화 시스템을 도입하기 위해서는 제조 공장이 갖는 보안 취약점과 개인정보 보호 문제는 반드시 선결해야만 한다. 그러므로 우리는 공장 자동화를 위해서 가장 많이 도입되고 있는 무선 통신 기술인 RFID 통신 프로토콜에 적용 가능한 경량 암호 프로토콜을 제안한다. 본 논문에서 제안한 경량 암호 프로토콜은 기존의 공개키 기반 시스템이나 대칭키 암호 알고리즘과 비교해서 연산 횟수가 적고 처리 속도가 빠르다. 뿐만 아니라 낮은 전력 소비량과 저장 공간을 소비하도록 설계하였다.

Low-weight Secure Encryption Protocol on RFID for Manufactory Automation

Deuk-Young Hwang*, Jin-Mook Kim**

ABSTRACT

There has been a growing interest in automation of factories in the country. And, the development in this regard has been actively attempted. In particular, on the basis of the "innovation 3.0 strategy of manufacturing industry", interest in the smart of the manufacturing plant of small and medium-sized enterprises has increased rapidly. As well as policy for building smart plant, technical, seeking a strategic approach. But, in order to introduce such a smart plant or factory automation systems, manufacturing plant security with vulnerability and personal information protection problems, it should always be top priority there. Accordingly, we provide the applicable lightweight secure protocols in RFID communication. It is a wireless communication technology that is most often introduced for factory automation. Our proposed lightweight secure protocol in this study, less the number of calculations in comparison with the existing public key-based and the symmetric key encryption algorithm. And it is fast in compare with the existing protocol. Furthermore, we design that it system can support to low power consumption and small consume the memory size.

Key words : IoT/CPS, RFID, Attribute-based Re-encryption, Industry standard, Smart factory

접수일(2016년 10월 01일), 수정일(1차: 2016년 12월 23일), 게재확정일(2016년 12월 27일)

★ 본 논문은 2015년 강원대학교 학술연구조성비 지원에 의하여 연구되었음(관리번호-201510037)).

* 강원대학교 삼척캠퍼스 / 컴퓨터공학과
** 선문대학교 / IT교육학부, 교신저자

1. 서 론

기존에는 PC와 서버를 중심으로 한 통신이나 데이터 처리가 중요 관심사였다[1, 2, 3, 4]. 하지만 최근에는 사물인터넷, 센서 네트워크, 가상 물리시스템, 클라우드 컴퓨팅 서비스 등의 발달로 인해서, 제조 공장에 대한 스마트화에 대한 관심이 급격하게 증가하고 있다. 특히, 국내에서는 2014년 '제조업 혁신 3.0 전략'을 발표하고, 국내 제조 공장에 대한 스마트화 사업을 중점적으로 확대하고자 노력하고 있는 실정이다[5].

하지만 공장 자동화 또는 스마트 공장을 구축함에 있어서, 기존의 PC 기반 통신 환경과 마찬가지로 여러 가지 선결해야만 하는 문제점들이 산재해 있다[6]. 특히, 제조 공장이 갖는 보안 취약점과 개인정보 보호, 기기에 대한 접근 제어에 문제는 반드시 선결되어야만 한다[7, 8, 10].

그러므로 본 논문의 저자들은 자동차 부품 제조공장을 대상으로 스마트 전자 브라켓(SEB)을 설계 및 제작하여 RFID와 WiFi 통합 네트워크를 무선으로 선행 연구로 수행하였다. 선행 연구한 스마트 전자브라켓에 탑재한 RFID 13.56Mhz 태그에 적은 저장 용량과 처리 속도를 고려하여 기존의 속성기반 암호 기술을 사용한 경량 암호 프로토콜을 설계하였다[9].

본 논문에서 제안한 공장 자동화를 위한 RFID 경량 암호 프로토콜은 속성기반 암호 알고리즘을 기초로 설계하였다. 그러므로 기존의 공개키 기반 암호 프로토콜이나 대칭키 기반 암호 프로토콜보다 연산 복잡도가 낮고, 권한 기반 장치 접근제어가 가능하다. 뿐만 아니라 기존에 사용하던 장치들에 대한 확장성을 고려해서 설계하였다.

2. 관련연구

2.1 스마트 공장을 위한 고려사항

국내 자동차 부품 제조 공장들은 대체로 영세하고, 기기나 설비 투자의 여유가 적거나 없으며, 국가의 시행 방침에 따라 스마트 공장으로 변형하기에 경제적, 인력적 제약을 가지고 있다. 두 번째로 제조 공장이라는 환경적 제약 사항으로 심한 소음과 진동, 먼지 등으로 인해서, Zigbee 대신 RFID 무선 통신 장치를 사용하는 것이 효과적이다[5, 8].

세 번째로 제조업의 업무적 특성상 작업자는 작업자의 시선 높이에 설치된 PPC에서 작업 지시사항을 숙지하고, 해당 작업을 정해진 시간 내에 처리해야만 한다. 이때 온도나 습도, 진동, 작업대의 정렬 등에 대해 측정한 센서 데이터들을 실시간으로 서버에 전달한 후, 이에 대한 작업 진행 순서, 작업 상황 제어, 생산 중 발생한 문제에 대한 해결방안 적용이 가능해야만 한다.

이외에도 저렴하고 크기가 작고 설치하기 쉬운 통신장치라고 하더라도 설치하기 편해야 하고, 작업자의 작업에 방해를 주지 않아야 하며, 안전사고를 미연에 방지할 수 있어야만 한다.

2.2 스마트 공장에서 발생 가능한 취약점

본 논문에서 제안하는 스마트공장에서 발생할 수 있는 취약점들을 다음과 같다[5, 6].

① 공장 내의 진동 및 소음 등으로 인한 무선 통신장치의 통신 문제 : 제조 공장에는 프레스와 같은 큰 진동이나 소음을 발생하는 기기들이 많다. 이로 인한 통신 오류 또는 장치에 대한 정당한 사용을 거부할 수 있다.

② 센서 및 통신 장치의 낮은 비용 : 각종 제조 공장에 별도의 정보 수집장치들은 저렴한 비용으로 제작 가능하고, 통신 도달

거리는 컨베이어 벨트 시스템을 고려해서 50m 이상의 무선 통신이 가능해야 한다. 특히, CPS(Cyber Physical System)의 특징상 각종 센서들을 통해서 수집된 정보들을 서버에 실시간으로 전달해야 한다.

③ 중간자 공격 : 각종 센서들이 수집한 제조 공정 관련 정보들을 중간에서 가로채어, 이를 위조하거나 악용하는 문제가 발생할 수 있다.

④ 작업자 또는 기기 가장 공격 : 스마트공장에서 근무하는 작업자 신분에 대한 가장공격 또는 공장 내 각종 장치들이 무선 통신으로 연결되어 있음을 악용한 기기 가장 공격이 가능하다.

2.3 속성기반 재-암호화 알고리즘

B. Water에 의해서 제안된 속성기반 암호 알고리즘은 정의된 Bilinear map을 기반으로 한다 [11, 12, 13, 14, 15].

- Bilinear : 임의의 군 원소는 g1, g2 ∈ G1와 a, b ∈ Z에 대해 가 성립된다.

- Non-degenerate ; g ∈G1의 생성원은 e(g,g) ≠ 1에 대해서 만족해야 한다.

- Computability : 임의의 생성원 G1에서 e(g1,g2)를 계산할 수 있는 알고리즘이 존재한다.

그리고 속성기반 암호 알고리즘은 5가지 처리 절차를 갖는다.

① Attribute Base Encryption Global Setup(GP,) -> Global Parameter : Security Parameter를 입력받은 후 Global Parameter를 생성한다.

② Attribute Base Encryption Auth Setup(GP,) -> {, } : 발급기관은 번째 키 Global Parameter를 입력받아 공개키/개인키를 생성한다.

③ Attribute Base Encryption Key Gen(GID, , u, GP,) -> , : 인증기관들은 사용자의 GlD기반으로 를 발급한다.

④ Attribute Base Encryption Encrypt(M, Q, ,GP) -> CT : 암호화를 수행하기 위해서 접근정책 Q,기관의 공개키 , Global Parameter 기반으로 암호문 Ciphertext를 추출한다.

⑤ Attribute Base Encryption Decrypt(Ciphertext, Q, ,GP) : 암호화된 속성 기반 암호문을 복호화한다.

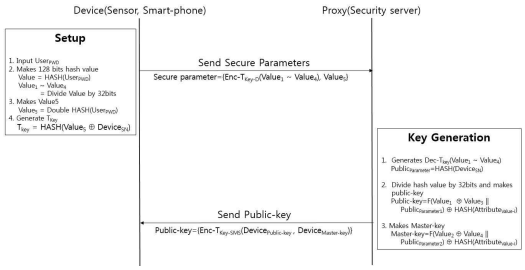
기존에 RFID와 같은 경량 시스템을 위해서 한국인터넷진흥원에서는 Light weight SEED와 같은 암호 알고리즘들을 제안하였다. 하지만 현실적으로 이를 그대로 적용하기에는 어려움이 많다. 그러므로 본 연구에서는 속성기반 암호 알고리즘을 적용함으로써 동작절차를 간소화하고, 처리시간과 소비전력을 낮출 수 있도록 하고자 한다.

3. 제안시스템

본 연구에서는 앞 절에서 살펴본 바와 같이 제조 공장이라는 특별한 환경 때문에 발생할 수 있는 취약점뿐만 아니라, 가상 물리시스템에서 사물인터넷 환경을 안전하게 구축해야 하는 한계 때문에 앞서 2.2절에서 기술한 바와 같이 4가지 취약점들이 발생한다. 그러므로 본 논문에서는 이와 같은 취약점들을 고려해서, 공장 자동화 환경에서 RFID를 사용한 가볍고 빠르게 동작할 수 있는 속성기반 암호 프로토콜을 제안한다.

3.1 키 생성 단계

사용자는 IoT Device를 사용하기 전 Secure Management Server에서 설정을 완료 후 공개키, 마스터를 생성 받은 후 등록 및 인증, 메시지 통신을 수행한다. 기존의 속성기반 암호화 방식에서 권한등급 값을 해쉬함수를 수행하여 접근제어 파라미터를 설계하였다. 사용자가 디바이스(Device)와 같이 프록시(Security Server)에서 공개키를 발급과정은 (그림 1)에 나타냈다.



(그림 1) 설정 및 키 생성 단계

1. 사용자는 디바이스(Device)에서 사용자가 알 수 있는 $User_{PWD}$를 입력 한다. 다음부턴 디바이스에서 해쉬함수를 사용해 128 비트 해쉬값을 생성한다.

$$Hash(User_{Pwd}) = Value$$

2. 생성된 해쉬값에 해쉬함수를 수행하여 보안 파라미터 값을 생성한다. 해쉬값을 수행하기 이전 생성된 128비트의 해쉬값을 32bit 단위로 4개로 구분하고, 각각의 값을 설정하였다. 생성된 파라미터 값들은 해쉬함수를 사용해서 생성한 후, $Value_1, Value_3$을 공개키로 사용하고, $Value_2, Value_4$를 비밀키로 설정한다. 다음으로 한 번 더 해쉬함수를 사용해서 사용자가 입력한 패스워드를 속성기반의 파라미터로 설정한 후 암호화해서 전송한다.

$$Value_i = Value_1, Value_2, Value_3, Value_4$$
$$HASH(HASH(User_{Pwd}) = Value_5$$

3. 이후 임시키를 생성 후 시큐어 파라미터를 프록시(Security Server)로 전송한다.

$$Enc_{-Tkey}(Value_{1\sim4}), Value_5$$

4. 프록시(Security Server)에서 수신한 메시지를 복호화 후 $Public_{Parameter}$를 생성한다.

$$Public_{Parameter}(HASH_{Device})$$

5. $Value_{1\sim4}$ 의 해쉬값들을 붙여서 128비트로 만든 후, 32비트씩 나눠서 공개키와 마스터키를 생성한다.

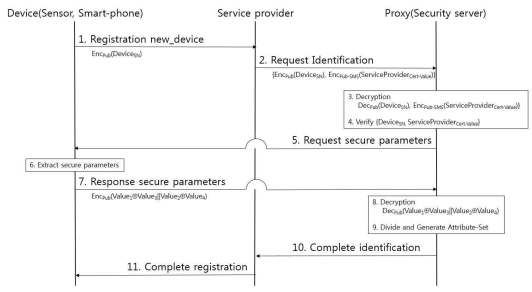
$$Master = F(Value_2 \oplus Value_4 \| Public_{parameter2}) \oplus Hash(attribute_{Value})$$

6. 생성된 공개키와 마스터키는 임시키를 생성 후 디바이스(device)로 전송한다.

$$Enc_{-Tkey-SMS}(Device_{public-key}, Device_{master-key})$$

3.2 디바이스 등록 단계

사용자는 IoT Device를 사용하기 전 Secure Management Server에서 설정을 완료 후 공개키, 마스터를 생성 받은 후 등록 및 인증, 메시지 통신을 수행한다. 디바이스 등록단계에 대한 프로토콜의 동작절차를 (그림 2)에 나타내었다.



(그림 2) 기기 등록절차

사용자가 디바이스를 프록시에 등록하는 단계를 수행하는 절차를 11단계로 나타내었다. (그림

2)에 나타낸 등록절차에 대해서 작업 단위로 구분해 설명하였다.

1. 디바이스를 서비스 제공자에게 등록한다. 다음으로 서비스 제공자는 자신의 식별기호를 포함해 프록시에 식별해 줄 것을 요청한다.

$E_{Pub}(Device_{SN})$

$E_{Pub}(Device_{SN}), E_{Pub-SMS}(ServiceProvider_{Cert-value})$

2. 프록시는 수신된 메시지를 복호화한다. 다음으로 디바이스의 시리얼 번호, 식별값의 타당성을 검토한다. 그리고, 디바이스에게 시큐어 파라미터를 요청한다.

$D_{Pub}(Device_{SN}), D_{Pub-SMS}(ServiceProvider_{Cert-value})$

Checking $Device_{SN}, ServiceProvider_{Cert-value}$

3. 시큐어 파라미터 요청을 받은 디바이스는 자신의 시큐어 파라미터를 암호화해서 프록시에게 전달한다.

$E_{pub}(Value_1 \oplus Value_3 \| Value_2 \oplus Value_4)$

4. 프록시는 수신한 시큐어 파라미터를 32비트 단위로 나눈 후, 식별 요청메시지에 대한 타당성을 검토한다.

$D_{pub}(Value_1 \oplus Value_3 \| Value_2 \oplus Value_4)$

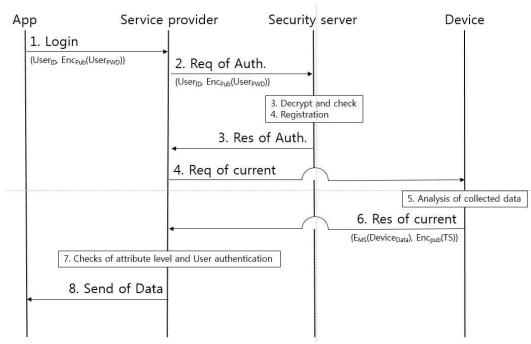
4. 프록시는 $nonce$를 생성 후, 서비스 제공자에게 식별 성공 메시지를 전송한다.

$E_{pub-SP}(Attribute_{Grade}, SMS_{nonce})$,
$E_{pri-sms}(SMS_{nonce})$

5. 서비스 제공자는 수신한 메시지를 복호화하고, $Device_{SN}$와 현재 시간, 디바이스 속성 값을 저장한다. 다음으로 기기 등록 성공 메시지를 전송한 후 통신을 마친다.

3.3 사용자인증 및 메시지통신 절차

등록된 디바이스를 활용하여 사용자가 스마트폰의 어플리케이션을 접속 후 디바이스로부터 수집된 메시지를 전송받는 단계이다. 사용자 인증 및 메시지 통신에 대한 프로토콜은 (그림 3)과 같다.



(그림 3) 사용자 인증 및 메시지인증 단계

메시지를 전송받기 전에 사용자 인증을 수행하여 식별하고 이에 등급에 알맞은 메시지를 전송한다.

1. 사용자는 등록된 디바이스를 사용하여 서비스를 요청한다.

$User_{ID}, E_{pub}(User_{Pwd})$

2. 서비스 제공자는 프록시에게 인증 요청 메시지를 전송한다. 그러면 프록시는 수신한 메시지를 복호화 하여 $User_{ID}, User_{Pwd}$를 검사한다. 그리고 정당한 사용자인 경우에만 사용자 정보를 서버에 등록한다.

3. 프록시는 사용자 인증 확인 메시지를 서비스 제공자에게 전송한다. 그리고 서비스 제공자는 디바이스에게 수집된 데이터를 전달해 달라고 요청한다.

4. 디바이스는 요청 받은 데이터를 분석 후, 서비스 제공자에게 수집한 데이터를 전송한다.

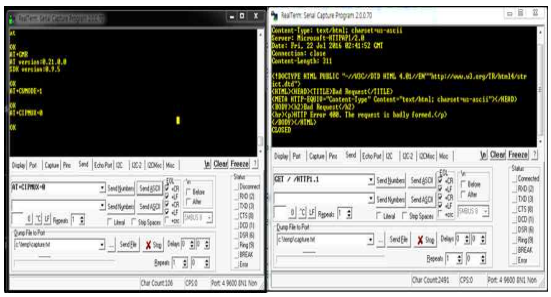
$E_{MS}(Device_{Data}), E_{Pub}(TimeStamp)$

5. 서비스 제공자는 수집된 데이터와 사용자의 속성 등급을 비교 분석한 후 정당한 경우에는 수집한 데이터를 전달한다. 다음으로 앱으로부터 데이터를 전송하기 전에 먼저 현재 시간값을 등록한다.

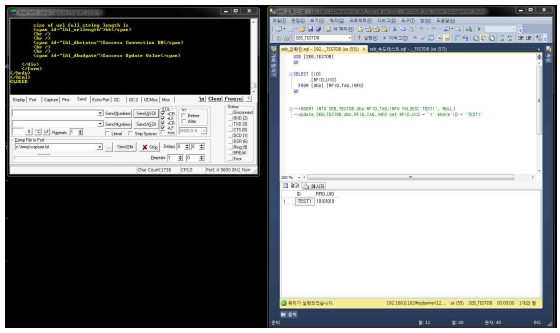
4. 비교 및 분석

4.1 정상적인 통신장치 동작시험

본 논문의 제안시스템이 올바르게 동작하는지 여부를 증명하기 위해서 공인인증시험기관인 TTA에 의뢰하여 응답지연시간과 정보수집능력에 대한 시험을 실시하였다. (그림 4)는 본 연구 논문에서 제작한 SEB의 통신 여부와 통신 응답 속도를 측정한 화면을 나타내었다.



(그림 4) AP 통신 테스트



(그림 5) 서버와 WiFi 모듈 동작 확인

(그림 5)는 WiFi AP를 사용해서 50m 이상 거리에 위치한 터미널 장치에서 통신이 원활하게 수행됨을 스캔한 화면이다. (그림 5)에 나타난 바와 같이, 재-암호화 알고리즘을 처리함으로 인해서 표준 통식속도보다 지연시간이 발생하였다. 하지만 정상적인 동작은 가능하다.

4.2 보안 서비스 분석

1. 인가되지 않은 사용자 접근제어 및 키 관리 : RFID를 탑재한 SEB는 비-인가된 사용자의 접근 및 도난/분실로 인해 장치의 제어권을 획득하여 장치를 오남용할 수 있는 사례가 발견되고 있다. 하지만 본 연구 논문에서 제안한 SEB는 장치의 접근제어를 강화하기 위해서 장치 설정 및 키 생성 단계에서 $Security_{Parameter}$를 등록된 장치에 발급하였다. 그리고 장치 등록과정에서 $Security_{Parameter}$를 검증 및 식별 메시지를 사용한 접근 차단 단계를 마련하였다.
   그러므로 제안 시스템은 비-인가된 사용자의 접근이 차단가능할 뿐만 아니라, 키 관리 프로토콜을 통해서 안전한 키 분배가 가능함을 보였다.
2. 세션 하이재킹 및 무결성 위협 : 통신 과정 중에 발생할 수 있는 세션 하이재킹을 통해서 디바이스들이 수집한 정보를 가로챌 수 있다. 이를 위해서 제안 시스템은 디바이스 간 식별 메시지와 OTP 성격으로 현재 시간

을 측정해서 오프셋으로 사용하였으므로 이를 원칙적으로 방지할 수 있다. 뿐만 아니라 사용자 인증 단계에서 디바이스 별로 공개키 및 마스터 키를 사용해서 재-암호화를 수행하므로 데이터 무결성을 보증할 수 있다.

5. 결 론

우리는 본 논문에서 인더스트리 4.0 정책에 부합하는 실시간성과 생산 효율성을 높일 수 있도록 SEB를 설계 및 제작하였다. 그리고 제안한 시스템에 속성기반 재-암호화 알고리즘을 적용해서 가볍고 빠르게 동작할 수 있도록 RFID에 탑재하였다. 그리고 해당 시스템의 동작범위를 넓히고자 WiFI망과 연동해서 통신을 수행한 결과를 보였다. 제안시스템은 공장자동화 환경에서 통신 범위를 넓힐 수 있을 뿐만 아니라 사용자 속성을 기반으로 가볍고 빠르게 동작하도록 재-암호화 프로토콜을 탑재함으로써 쉽고 안전하게 기계 제어 및 사용자 인증에 활용할 수 있다.

기존에 경량 암호들을 RFID 시스템에 적용함에 소비전력이나 저장용량의 제한적인 문제들을 해결하고자 속성기반 재-암호 알고리즘을 적용함으로써 저-전력, 소-용량 RFID 시스템에서도 만족할 만한 처리 능력을 보장할 수 있도록 하였다.

ACKNOWLEDGMENTS

This study was supported by 2015 Research Grant from Kangwon National University(No. 201510037).

참고문헌

[1] Dong Chen, Guiran Chang, A Survey on Security Issues of M2M Communications in Cyber-Physical Systems, KSII Transactions on Internet and Information(TIIS), Vol. 6, No. 1, pp.24-45, 2012. 1.

[2] Jiafu Wan, Hehua Yan, Hui Suo, Fang Li, Advances in Cyber-Physical System Research, KSII Transactions on Internet and Information(TIIS), Vol. 5, No. 11, pp.1891-1908, 2011. 11.

[3] Dae-Geun Kim, Man-Gon Park, Horizontal Integration between Cyber Physical System Based on Industry 4.0 and Manufacture Execution Systems through Middleware Building, Journal of Korea Multimedia Society, Vol. 17, No. 12, pp.1484-1493, 2014. 12.

[4] Young-Sik Kim, Cyber-Physical System Security Technology Trend in IoT era, The Magazine of the IEEE, Vol. 42, No. 8, pp.16-25, 2015. 8.

[5] Jae-Hyun Lim, German, Again Industry 4.0, Journal of Korea Association of Machinery Industry, Vol. 45, No. 7, Total-vol. 457, pp.34-39, 2015. 7.

[6] Armin Puhringer, Impact on the existing industrial communication on the IoT and Industry 4.0, Monthly ICN, Total Vol. 105, pp 22-27, 2015. 11.

[7] Ray Y. Zhong, Huajun Gong, Chen Xu, and Shaoping Lu, Physical Internet-Enabled Manufactureing Execution System for Intelligent Workshop Production, International Journal of Signal Processing, Image Processing and Pattern Recofnition, Vol. 9, No. 6, pp.121-132, 2016.

[8] Ok-Jae Lee, A Design of Automatic Management System in Manufacturing Process of Semiconductor Package Elements by Using RFID, The Jorunal of The Korean Institute of Communication Science, Vol. 33, No. 8, pp.313-320, 2008. 8.

[9] Zhixin Yang, Pengbo Zhang, Lei Chen, RFID-enabled indoor positioning method for a real-time manufacturing execution system using OS-ELM,

[10] Francisco Almada-Lobo, The Industry 4.0 revolution and the future of Manufacturing Execution System(MES), Journal of Innovation

Management, Vol. 3, No. 4, pp16-21, 2015.

[11] Kwangyong Park, Youjin Song, Attribute-based Encryption Technique, REVIEW OF KIISC, Vol.20. No.2, 85-92, 2010.4

[12] Jongho Moon, Younsung Choi, Dongho Won, A Secure Attribute-based Authentication Scheme for Cloud Computing, KIISE Transactions on Computing Practices, Vol. 22, No. 8, pp. 345-350, 2016. 8.

[13] Hye-Joung Yoo, Attribute-Based Authenentication for Secure Cloud Computing, Journal of KIIT, No.13, No.1, pp.59-69, 2015. 1.

[14] Soomi Yang, An Efficient Attribute Certficate Management Technique for Highly Distributed Environment, Jouranl of Information and Security, Vol. 5, No.1, pp.85-92, 2005.3.

[15] Si-Choon Noh, A Study of DES Property, Diagnosis and How to Apply Enhanced Symmetric Key Encryption Algorithm, Jouranl of Information and Security, Vol. 12, No.4, pp.85-90, 2012. 9.

[著 者 紹 介]

황 득 영 (Deuk-Young Hwang)
1988년 2월 : 광운대학교 전자계산학과(이학사)
1990년 2월 : 광운대학교 전자계산학과(공학석사)
1999년 2월 : 광운대학교 전자계산학과 (공학박사)
1990년 3월 ~ 1994년 2월 : 전주 기전대학교 전자계산학과 조교수
1994년 3월 ~ 현재 : 강원대학교 삼척캠퍼스 컴퓨터공학과 교수
관심분야 : 프로그래밍 언어, 컴파일러, 정보보안, 빅-데이터
email : dyhwang@kangwon.ac.kr

김 진 묵 (Jin-Mook Kim)
1998년 2월 : 배재대학교 전자계산학과(이학사)
2000년 2월 : 배재대학교 컴퓨터공학과(공학석사)
2006년 2월 : 광운대학교 컴퓨터과학과(공학박사)
2006년 9월 ~ 2008년 2월 : 선문대학교 컴퓨터공학과 연구교수
2006년 9월 ~ 현재 : 선문대학교 IT교육학부 부교수
관심분야 : 정보보호, 네트워크 보안, 사용자 인증, 빅-데이터 분석
E-Mail : calf0425@sunmoon.ac.kr