Regular paper

Journal of the KIECS. pp. 243-250, vol. 14, no. 1, Feb. 28. 2019, t. 93, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2019.14.1.243

정보보호 필요에 따른 클라우드 기반의 안전한 파일관리 보안솔루션 연구

김희철*

A Study on Cloud-Based Secure File Management Security Solutions According yo Information Protection Needs

Hee-Chul Kim*

요 약

본 연구는 클라우드 환경에서 매체기반의 SFMS(: Secure File Management Security) 개발을 통하여 블루투스 기반의 암호모듈을 이용하여 컴퓨터에서 클라우드 데이터를 암·복호화 한다. 블루투스 암호모듈은 클라우드에 저장된 파일을 손쉽게 열람 가능하지만 모듈이 없으면 절대 열람이 불가능하다. 최근 이슈화 되고 있는 해킹이나 개인자료유출 등의 문제점을 근본적으로 차단하는 솔루션이라 할 수 있다.

ABSTRACT

In this paper, we develop a Secure File Management Security(: SFMS) based on media in a cloud environment to encrypt and decrypt cloud data on a computer using a Bluetooth - based cryptographic module. The Bluetooth cipher module makes it easy to browse files stored in the cloud, but it is never possible to browse without a module. It is a solution that fundamentally blocks the problems such as hacking and leakage of personal data that have recently become an issue.

키 워드

Secure File Management Security, Hacking, Security As A Service, Big Data, Cloud
SFMS, 해킹, SEcaaS, 빅데이터, 클라우드

Ⅰ. 서 론

오늘날 매체 및 네트워크 발전에 따른 클라우드 서비스의 기술 발달은 시간과 공간의 제약을 벗어난 정보 서비스의 제공이 가능하고 개인정보의 보관과 이동 및 수집·처리가 매우 간편하고 용이해졌다. 반면에, 해킹 및 개인정보 유출로 인한 개인과 기업은 국가적으로 손실이 점점 커지고 있는 상황이다.

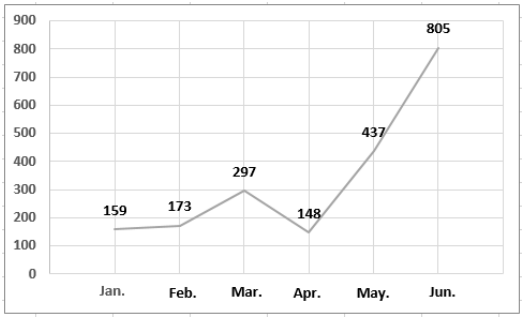
본 연구는 클라우드 환경에서 매체기반의 안전한 파일관리 보안시스템 개발을 통하여 블루투스 기반의 암호모듈을 이용하여 컴퓨터에서 클라우드 데이터를 암·복호화 한다[1].

표1 은 한국랜섬웨어침해대응센터에서 제공하는 2016년 상반기 랜섬웨어 침해신고 피해 건수로 총

* 교신저자 : 광주대학교 컴퓨터공학과
· 접 수 일 : 2018. 12. 13
· 수정완료일 : 2019. 01. 14
· 게재확정일 : 2019. 02. 15
· Received : Dec. 13, 2018, Revised : Jan. 14, 2019, Accepted : Feb. 15, 2019
· Corresponding Author :Hee Chul Kim
Dept. Gwang-Ju University,
Email : jaziri@daum.net

2019건으로 3월부터 12월까지 집계한 수치(2678건)이다. 1월 159건에서 3월에는 297건으로 2배 가까이 늘었고, 5월에는 437건, 6월에는 805건으로 급증했다.

표 1. 2016년 상반기 랜섬웨어 월별 침해통계
Table 1. Monthly infringement statistics of Ramsome ware by the first half of 2016



개인정보 유출사례에서 발생한 랜섬웨어 건수를 보더라도 지속적으로 피해 사례는 늘어나고 있으며, 이러한 문제점을 해소하기 위해서 본 과제의 결과물 활용이 절실히 요구되어 질것으로 판단된다.

본 논문의 구성은 다음과 같다. 먼저 본 서론에 이어 2장에서는 SFMS의 H/W와 S/W에 대하여 간단히 살펴보고자 한다. 3장에서는 SFMS 보안솔루션 개발에 대하여 기술하고자 한다. 4장에서는 블루투스 인터페이스 암호모듈 및 SFMS모듈에 운영되는 응용 S/W체제에 대해 고찰하고 마지막으로 5장에서 결론을 맺고자 한다.

II. 시스템 구성

SFMS에서 그림 1은 블루투스 암호모듈을 바탕으로 각종 전산기뿐만이 아니라 클라우드 내부 데이터를 자신의 블루투스 암호모듈(암호키)을 이용하여 전산 데이터를 보호함으로써 전산기 또는 클라우드 내부에 저장된 데이터를 보호하기 위한 솔루션이다. 여기서 암호키는 별도로 존재하고 암호화하는 당시에 암호키가 생성되며 윈도우즈, 안드로이드, 아이폰, 맥 복에서 자신의 자료의 암호화 및 클라우드 데이터를 암호화하여 저장하고 복호화 시에는 자신이 가지고 있는 모듈을 통해서만 열람이 가능함으로 어느 누구도 모듈이 없는 상태에서는 파일 열람이 불가능하다는 장점이 있다[2-3].

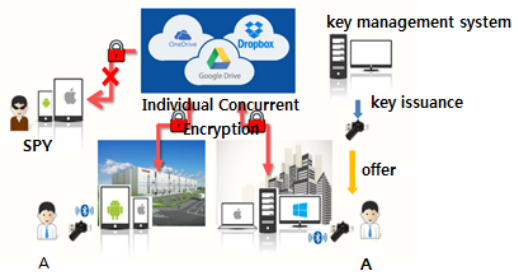


그림 1. 블루투스 암호모듈 구성도
Fig. 1 Bluetooth password module configuration

또한, 사용자가 가지고 있는 블루투스 암호모듈은 클라우드에 저장된 파일을 손쉽게 열람 가능하지만 모듈이 없으면 절대 열람이 불가능하며 자신의 모듈이 아닌 다른 모듈은 절대 접근이 불가능함으로 최근 이슈화 되고 있는 해킹이나 개인자료유출 문제점을 근본적으로 해결 가능한 솔루션이라 할 수 있다.

2.1 H/W 구조

H/W 구조는 그림 2와 같이 전산기를 기반으로 암호모듈이 블루투스를 이용하여 연동되며 다양한 디바이스를 공통적으로 사용 가능하도록 관련 기능을 개발하였다[4].

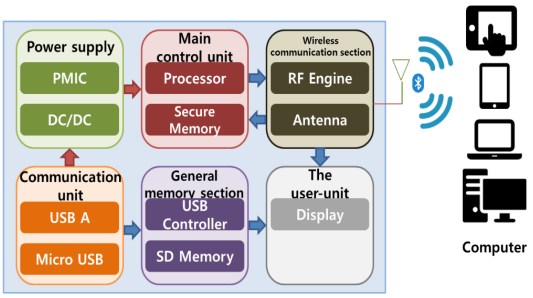


그림 2. 블루투스 기반 H/W 구조도
Fig. 2 Bluetooth-based H/W structure

2.2 S/W 구조

S/W 구조는 각종 전산기(Windows(MAC),

Android (iOS))에 기본적으로 Client S/W가 탑재되며 암호모듈간은 블루투스 통신을 이용함으로 드라이버 단은 블루투스 드라이버 및 Crypto API가 연동되고 상위 계층은 자동/수동암호화, 백업 기능, 파일관리기능, 사용자 관리 기능이 위치하고 Cloud와는 IP 네트웍을 통해 연동되며 기본 구조는 아래 그림 3과 같다.

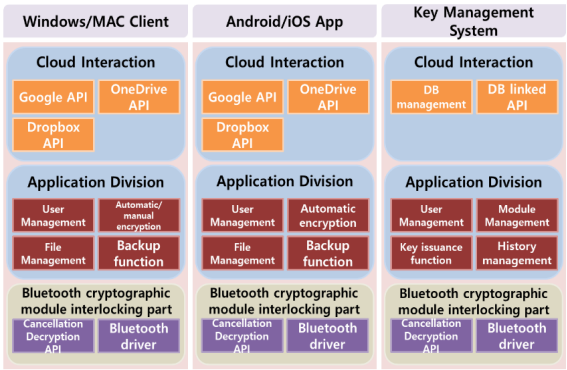


그림 3. 블루투스 기반 S/W 구조도

Fig. 3 Bluetooth-based S/W structure

III. 파일관리 보안 솔루션 개발

3.1 블루투스 암호모듈 H/W 개발

H/W 구조는 전산기를 기반으로 암호모듈이 블루투스를 이용하여 연동되며 다양한 디바이스를 공통적으로 사용 가능하도록 관련 기능을 탑재하고, 하드웨어 구성요소들의 기능 및 구성, 외부 인터페이스 규격 및 블록들 간의 인터페이스에 관하여 기술한다[5].

3.1.1 블록의 기능 규격 및 인터페이스 규격

블록 기능으로 크게 제어부, 무선 통신부, 전원부로 구분된다. 제어부는 USB2642 USB HUB to SD Controller를 사용하여, BLE칩 USB 연결 기능을 하며, Micro SD 메모리를 USB에 연결하여 사용 및 제어가 가능하다. LED 램프를 통해 Micro SD 메모리 동작 상태를 표시한다. 그리고 Micro-USB combo USB-A Connector를 사용하여 사용자 편의에 따라 USB 연결이 가능하도록 설계했다. 또한, 무선 통신부는 CC2540 Bluetooth Low Energy를 사용하여 외부 장비간 무선 통신할 수 있도록 전기적 신호로 변환 가능하도록 설계했다. 그리고 제어부와 USB I/F 방식을 사용하여 USB 연결이 가능하도록 설계했다. 전원부는 USB포트를 통해 공급되는 DC 5V 전원을 공급받아 LDO를 각각 사용하여 3.3V로 변환하여 제어부와 무선 통신부에 전원을 공급해 주도록 그림 4와 같이 제작했다[6].

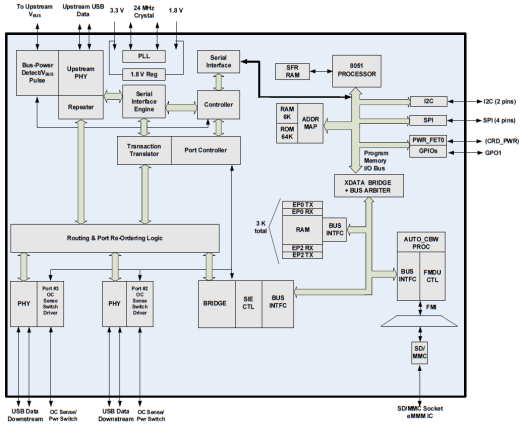


그림 4. USB2642 Block Diagram

Fig. 4 USB2642 Block Diagram

3.2 블루투스 암호모듈 S/W 개발

BLE는 종종 Bluetooth Smart로도 불리며 classic bluetooth의 경량화 버전을 목표로 블루투스 4.0으로 Classic bluetooth와 겹치는 부분이 존재하지만 BLE는 완전히 다른 표준으로 블루투스 표준화 그룹인 Bluetooth SIG에 의해서 개발되기 전까지 Nokia의 사내 프로젝트(Wibree)로 시작하였다.

3.2.1 GAP

GAP는 Generic Access Profile의 약자로 블루투스에서 게시(advertising)와 연결(connection)을 제어한다. GAP은 특정 장치가 다른 장치들에게 어떻게 보이도록 할 것인가와 어떻게 두 장치를 연결할 것인가를 결정한다. GAP은 장치들이 맡을 수 있는 다양한 역할들에 대해 정의한다. 그 중 가장 핵심이 되는 컨셉은 Central 장치와 Peripheral 장치입니다. Peripheral 장치는 주로 작고, 저전력으로 동작하고, 제한된 리소스를 가진 장치들로 보다 리소스가 풍부한 Central 장치에 연결되어 동작하도록 설계된 장치이다. Heart Rate Monitor(심박측정기), BLE 근접센

서 태그 등이 해당된다. Central 장치는 폰이나 태블릿과 같이 충분한 전원과 메모리 등의 리소스를 갖춘 장치다[7].

3.2.2 ADVERTISING AND SCAN RESPONSE DATA

GAP을 이용해서 게시(Advertising)를 할 때 Advertising Data Payload와 Scan Response Payload를 포함할 수 있다. 두 가지는 서로 구분되며 31바이트까지 데이터를 포함할 수 있다. 하지만 Advertising Data Payload가 필수인데 반해 Scan Response Payload는 선택적이다. Advertising Data Payload는 Central 장치가 인식할 수 있도록 peripheral 장치에서 계속 송출되는 데이터다. Scan Response Payload는 central 장치에서 장치 이름과 같이 추가적인 정보를 요구하기 위해 정의된 것으로 선택적으로 구현된다. Advertising 과정이 어떻게 동작하는지는 그림 5에서 보여준다[8].

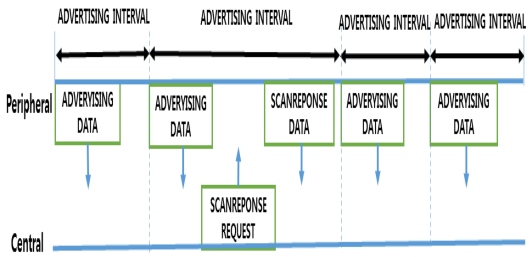


그림 5. Advertising 과정
Fig. 5 Advertising course

먼저 Peripheral 장치는 특정한 게시 주기(advertising interval)를 가지고, 주기마다 advertising packet을 전송한다. 주기가 길어질수록 전력소모를 줄여주지만 Central 장치에서의 반응이 느려진다. 만약 수신 장치(central 장치)에서 Scan Response Data 에 관심이 있다면 추가로 요청을 보낼 수 있고 peripheral 이 여기에 데이터와 함께 응답한다.

3.2.3 BROADCASTING, BEACON

Peripheral 장치는 31바이트의 작은 데이터를 실어서 게시(advertising)를 함으로써 낮은 비용으로 주변의 central 장치에 자신의 존재를 알릴 수 있다. BLE에서는 이것을 Broadcasting 이라고 부른다. 그리고 advertising 역할만을 하는 Peripheral 장치가 바로 비컨(Beacon)이다. 애플의 iBeacon은 advertising packet의 custom payload 내용을 특정한 형식으로 작성하도록 정의한다.

일단 Central, Peripheral 두 장치가 연결되면 advertising은 종료되어 외부 장치에서 scan 되지 않는다. 이제 GATT 서비스와 특성(characteristic)을 사용하여 양방향으로 통신하게 된다.

3.3 SFMS모듈 운용 구조

SFMS 모듈은 기본적인 H/W 초기화를 수행한 다음 모듈을 사용하기 위해 ID와 Password를 기다린다. 그림 6은 단말기로부터 정상적으로 요청되면 모듈이 가지고 있는 ID와 Password를 확인하고 OK/NOK를 전달하여 응용 프로그램의 사용자 접근제어가 가능하도록 도움을 준다[9].

또한, 암·복호화 과정의 단말에서 암·복호화를 위한 키가 요청되면 모듈 내부에 생성된 Key 값을 제공하여 암·복호 수행되도록 지원한다. 암호키는 여러개를 확보하고 있다가 랜덤한 Index를 만들고 항상 사용자에게 랜덤한 암호키가 제공되도록 관련 기능을 구현하였다[10].

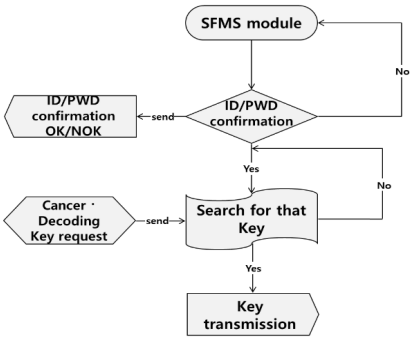


그림 6. SFMS 모듈 운용 구조
Fig. 6 SFMS module operation structure

Ⅳ. 구현 및 성능평가

4.1 블루투스 인터페이스 암호모듈 개발

그림 7은 USB2642의 인터페이스 중 SPI Flash에 제공되어 지는 SPI를 도시한 것으로 USB2642칩의 Serial number, Product 등 셋팅을 변경하기 위한 용도로 사용되고, UART 인터페이스는 CC2540의 UART 인터페이스의 Block으로 Debug용으로 사용된다. USB 인터페이스는 CC2540의 USB 인터페이스 Block으로 USB2642의 HUB를 거쳐 PC에서 사용된다.

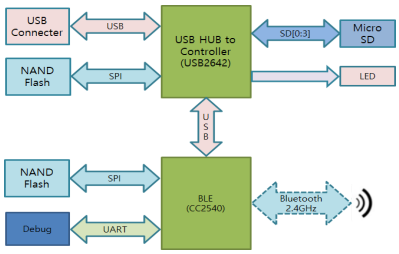


그림 7. 기능간 인터페이스 블록
Fig. 7 Inter-functional interface block

그림 8은 Bluetooth Interface를 나타내며 CC2540 Bluetooth에서 제공되는 RF를 사용하여 구성되며 보정회로 및 Antenna와 정합한다. 주파수는 2.4GHz 대역을 사용한다. Micro SD Interface는 USB2642에서 제공되는 SD 인터페이스를 사용하여 구성되며 Micro SD Connecter와 정합한다.

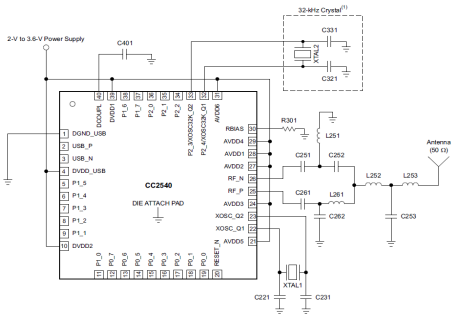


그림 8 블루투스 블럭
Fig. 8 Bluetooth Block

4.2 운영체제별 S/W 개발

개발된 S/W는 아래의 순서에 의해 동작된다. 첫 번째 로그인 요청하고 응답에 따라 후속 처리를 하며, 암호화 과정은 파라메타로 현재 시간을 넣어주면 Key 생성/검색과정을 거쳐 Key 값과 Index 값을 단말로 제공한다. Key 값을 가지고 암호화 과정을 수행하고 암호화가 완료되면 Index값을 파일에 저장한다. 복호화 과정은 암호화를 반대로 파일에 저장된 Index 값을 모듈에 넘겨주면 Key값을 다시 알려주어 복호화 Key가 전달되고 복호화 Key를 가지고 파일을 복호화 한다. 그림 9에서는 복호화 과정을 모두 완료하면 평문의 파일이 제공되는 과정을 나타낸 것이다.

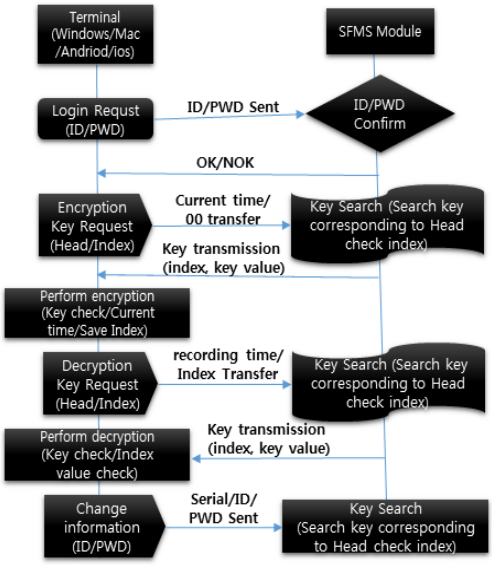


그림 9. S/W 기능 상세도
Fig. 9 Detail of S/W function

SFMS모듈에 운용되는 SW는 기본적으로 4개의 단말과 연동되며 그 대상은 Windows 프로그램, 안드로이드 앱 프로그램, MAC용 프로그램, 아이폰 앱 프로그램으로 나타낸다. 알고리즘의 통일화를 위해서 KISA가 배포한 ARIA-CBS알고리즘을 이용하였으며 호환성 TEST를 위해 각 단말별 암·복호 연동을 상호 교환하면서 시험을 한다.

4.2.1. Windows OS

사용자의 선택에 의해 “사용자 설정” 버튼을 누르면 아래와 같이 암복화 폴더 위치 변경이 가능하고, 클라우드 환경선택, 비밀번호 변경 바로가기가 가능하도록 관련 기능을 개발하였다.

또한, 암복호 위치는 기본적으로 자동 암호화 폴더로서 선택에 의해 변경이 가능하고 윈도우 탐색기를 이용하여 파일을 드래그를 통해 마음대로 이동이 가능하도록 관련 기능을 개발하였다.

클라우드는 Dropbox, OneDrive, Google Drive 총 3가지 폴더 연결이 가능하다. 그리고 로그인 상태에서 비밀번호 변경이 가능하다. 비밀번호 변경 후에는 꼭 SFMS 모듈을 탈착 후 재장착하여야 정상적으로 로그인이 가능하다.

윈도우져는 파일 선택 후 오른쪽 마우스를 눌러 Shell Script를 이용하여 파일 암호화/복호화가 가능하며 아래 그림처럼 메뉴가 나오면 선택에 의해서 파일 암복호 기능이 수행되도록 관련 기능을 개발하였다. 암호화된 파일은 확장자 끝에 Sec가 붙는다.

4.2.2 Android OS

Android에서 블루투스 암호모듈을 SFMS로 표기한다. 실행 App을 클릭 하면 프로그램이 실행되고, App에 대한 아이콘으로 표기한다. 화면 하단에는 데이터 사용에 대한 안내 문구가 있으며, 기본적으로 데이터를 사용하지 않으나 클라우드 기능을 사용시 데이터를 사용하게 된다. 비밀번호 변경은 로그인 화면에서 비밀번호 변경하기 위치에 버튼을 눌러 아이디, 현재 비밀번호와 새 비밀번호를 입력하고 변경하도록 관련 기능을 개발하였다. 비밀번호 변경 후에는 꼭 SFMS 모듈을 탈착 후 재장착하여야 정상적으로 로그인이 가능하다.

4.2.3. MacBook OS

로그인 화면 아래 비밀번호 변경하기를 누르면 비밀번호 변경 화면이 뜬다. 아이디, 현재 비밀번호, 새로운 비밀번호 확인을 거쳐서 승인을 누르면 비밀번호가 변경이 되도록 관련 기능을 개발 하였다. 비밀번호 변경 후에는 꼭 SFMS 모듈을 탈착 후 재장착하여야 정상적으로 로그인이 가능하다. MacBook은 파일 선택 후 오른쪽 마우스를 눌러 Shell Script를 이용하여 파일 암호화/복호화가 가능하며 아래 그림처럼 메뉴가 나오면 선택에 의해서 파일 암복호 기능이 수행되도록 관련 기능을 개발하였다. 암호화된 파일은 확장자 끝에 Sec가 붙는다.

4.2.4. iPhone OS

아이폰에서 블루투스 암호모듈을 SFMS로 표기하였으며 이미지는 아래와 같다. 실행 App을 클릭 하면 프로그램이 실행된다. 로그인 화면에서 아이디와 비밀번호를 입력 후 로그인 버튼을 누르면 아이디/비밀번호가 일치할 경우 Main 화면으로 진입하며, 만일 오류 발생 시에는 절대 메인화면으로 들어가지를 못하도록 관련 기능이 개발 되었다.

Ⅴ. 결 론

전산기나 단말기 내부 중요 자료에 대한 정보보호와 클라우드 내부 데이터에 대한 정보보호 기능을 개발하여 해킹에 의한 유출을 근본적으로 차단한다. 블루투스 기반 암호모듈을 개발하여 단말기와 사용자 인증을 거쳐 지정된 사용자만 사용가능하도록 접근제어 기능을 제공하고, 응용 SW(Windows, 안드로이드 앱, MAC용, 아이폰 앱) 프로그램으로 파일 이동만 하면 자동적으로 암호화 하는 기능을 수행한다.

블루투스 기반 정보보호모듈은 다양한 단말환경에 연동 가능하도록 개발되었으며 국내 최초이고 세계적으로도 이렇게 다양한 단말과 연동하는 정보보호 모듈은 존재하지 않고 있다. 클라우드 기반으로 한 서비스형 보안인 ‘SEcaaS(Security as a Service)’를 도입하고 있는 상황에서, 한국의 클라우드 보안 시장안정화 등 USB 보안모듈의 국산화로 수입 대체 효과가 예상된다.

감사의 글

이 연구는 2019년도 광주대학교 대학 연구비의 지원을 받아 수행되었음

References

[1] D. Boneh and B. Waters, “Conjunctive, Subset and Range Queries on Encrypted Data,” Theory of Cryptography Conf., Osaka, Japan, July, 2007, pp. 1-29.

[2] H. Lee and J. Oh, “Design and Implementation of a Small Server Room Environment Monitoring System by Using the Arduino,” *J. of the Korea Institute of Electronic Communication Sciences,* vol. 12, no. 2, Apr. 2017, pp. 386-387.

[3] D. Ryu and T. Choi, “Development of Open IoT platform based on Open Source Hardware & Cloud Service,” *J. of the Korea Institute of Electronic Communication Sciences,* vol. 11, no. 5, May 2016, pp. 485-49.

[4] K. Nam, “A Study on the Office Management Service Platform based on M2M/IoT,” *J. of the Korea Institute of Electronic Communication Sciences,* vol. 9, no. 12, Dec. 2014, pp. 1405-1413.

[5] D. Ryu and T. Choi, “Development of Open IoT platform based on Open Source Hardware & Cloud Service,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 5, Mar. 2016, pp. 485-490.

[6] H. Huh and J. Lee, "A Study on Development of H8 MCU IDB(Integrated development board) for Embedded Education," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 4, no. 1, 2009, pp. 51-57.

[7] K Yoo and D. Ko, “Study on the Performance Test Technique of Open SW-based Cloud computing.” *J. of Korean Institute of Information Technology*, vol. 10, no.7, 2012, pp.185-192.

[8] J. Saidov, B. Kim, J. Lee, and G. Lee, “Hardware Interlocking Security System with Secure Key Update Mechanisms In IoT Environments,” *J. of the Korea Institute of Electronic Communication Sciences,* vol. 12, no. 4, 2017, pp. 671-678.

[9] J. Jang, C. Choi, and D. Kim, “Design of Smart Tourism in Big Data,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 12, no. 4, 2017, pp. 637-644.

[10] J. Jang, D. Kim, and C. Choi, “Study on Hybrid Type Cloud System,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 6, 2016, pp. 611-618.

저자 소개

김희철(Hee-Chul Kim)

1990년 조선대학교 대학원 컴퓨터공학과 공학석사
2003년 조선대학교 대학원 컴퓨터공학과 공학박사
1982년 ~1985년 육군통신장교 중위 전역
현재 광주대학교 컴퓨터공학과 교수
2012년 ~현재 광주광역시 사회적기업 네트워크 운영위원
2012년 ~현재 광주광역시 지방건설기술심의위원회 평가위원
2013년 ~현재 전라남도 지방건설기술심의위원회 평가위원

※ 관심분야 : RFID/USN, 임베디드시스템, IoT, 신재생에너지, 네트워크 분석 및 설계