Journal of Convergence for Information Technology
Vol. 9. No. 1, pp. 142-150, 2019
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2019.9.1.142

A Study Medium-based safe File Management Security System on the cloud Environment

Hee-Chul Kim
Professor, Division of Computer Engineering, Gwangju University

클라우드 환경에서 매체기반의 안전한 파일관리 보안 시스템에 대한 연구

김희철
광주대학교 컴퓨터공학과 교수

Abstract This study is a file management security system that encrypts and decrypts computer and cloud data by using Bluetooth based cryptographic module. It is a necessary solution in terms of abuse of personal information and protection of social and national information. We developed H/W and S/W for SFMS(: Safe File Management Security) related Bluetooth module in cloud environment and implemented firmware development, encryption key generation and issuance, client program for system mobile and key management system. In the terminal internal encryption and decryption, SFMS was developed to ensure high security that the hacking itself is not possible because key values exist separately for each file.

Key Words : Cloud Computing, Image Encryption System, Ransomware, SFMS, Hacking

요 약 본 연구는 블루투스 기반의 암호모듈을 활용하여 전산기 및 클라우드 데이터를 암·복호화 하는 파일관리 보안시스템으로 개인정보의 오남용과 사회적, 국가적 정보보호 측면에서 반드시 필요한 솔루션이다. 클라우드 환경에서 SFMS(; Safe File Management Security) 관련 블루투스 암호모듈에 대한 H/W와 S/W를 개발하여 펌웨어 개발과 암호키 생성 및 발급, 시스템 모바일용 Client 프로그램, 키 관리 시스템 등을 적용하였다. 단말 내부 암·복호화는 파일별로 키값이 별도로 존재함으로 해킹 자체가 원천적으로 불가능 한 높은 안전성을 확보할 수 있는 SFMS 개발하였다.

주제어 : 클라우드 컴퓨팅, 이미지 암호화 시스템, 랜섬웨어, SFMS, 해킹

1. Introduction

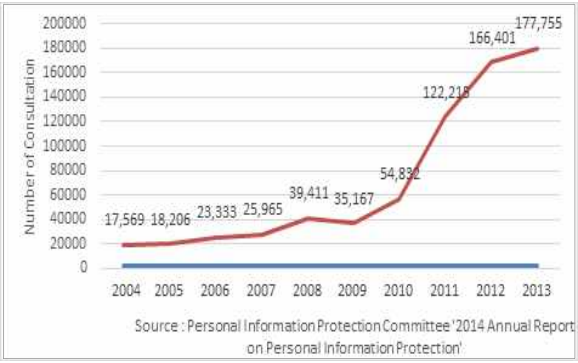
As computer technology is introduced in all fields today and the terminal itself is rapidly developed, leakage of personal information stored in the cloud / server inside the terminal is serious.

Table 1 below shows that in 2011, the number of cases of personal information infringement by year increased to more than

*This study was conducted with the support of Gwang-ju University Research Fellows in the 2019 academic year.
*Corresponding Author : Hee-Chul Kim(jaziri@daum.net)
Received November 19, 2018
Revised December 3, 2018
Accepted January 20, 2019
Published January 28, 2019

120,000, more than twice that of 54,000 in 2010. In 2012, there were 166,000 cases of personal information infringement did.

Table. 1 Personal Information Infringement Report by Year



The number of cases of ransomware in the case of personal information leakage has been continuously increasing, and it is expected that the use of the results of this study will be required to solve these problems in the future[1,2].

In this paper, we propose a secure media management system In Chapter 2 related research, In Chapter 3 Design and Method, In Chapter 4 Experiments and results are derived. Finally, we conclude this paper with conclusions and future research in Chapter 5.

2. Related reserarch

Based on the Bluetooth-based cryptographic module, it protects the data in the cloud using its own Bluetooth cryptographic module (encryption key). When a spy approaches for hacking, it uses the Bluetooth cipher module and encrypts it when it tries to leak and use internal data of cloud or internal data of computer.

This is because it is impossible to decrypt itself and important data is secured in the cloud environment by the user's request in preparation for the Ransomware. In the key management system, critical resources for key generation are injected and issued to the cryptographic module.

The key is basically generated and supplied by the random value when required by the computer. We have studied a related function that a separate encryption key is applied to every file, index is used to match the key for decryption, and the key is automatically searched if only the index stored in decryption is requested.

Users have studied related functions to be able to use regardless of computer or cloud environment and to enable encryption regardless of file format. It develops a Bluetooth-based crypto module and links it with a computer (laptop, Android smartphone, iOS phone, MACBook) and keeps access control and encryption/decryption function in the client program in the cloud. It can protect important personal information stored in the cloud environment and enter the market with an encryption device that can prevent leakage from the communication section.

3. Materials and Methods

3.1 Development of Bluetooth Code module H/W

The H/W structure is based on a computer, the cryptographic module is linked using Bluetooth, and related functions are mounted so that various devices can be commonly used. The hardware components study the function of the block and the external interface standard for the encryption file storage of the cloud service using the Bluetooth/USB cryptographic module.

3.1.1 Block Function and Interface Specification

It is divided into a control part, a wireless communication part, and a power part as a

block function. Fig. 1 uses the USB2642 USB HUB to SD Controller as the USB2642 Block Diagram as the controller. BLE chip USB connection function, Micro SD memory is connected to USB for use and control. BLE chip USB connection function, Micro SD memory is connected to USB for use and control. Display the micro SD memory operation status through LED lamp. And it is designed to enable USB connection according to user's convenience by using Micro-USB combo USB-A connector.

The wireless communication part is designed to be able to convert to electrical signal for wireless communication between external Equipment using CC2540 Bluetooth Low Energy. And it is designed to enable USB connection using the control unit and USB I/F method.

The power supply unit is designed to supply power to the control unit and the wireless communication unit by converting the power supply to 3.3V by using the LDO supplied with the DC 5V power supplied through the USB port[3,4].

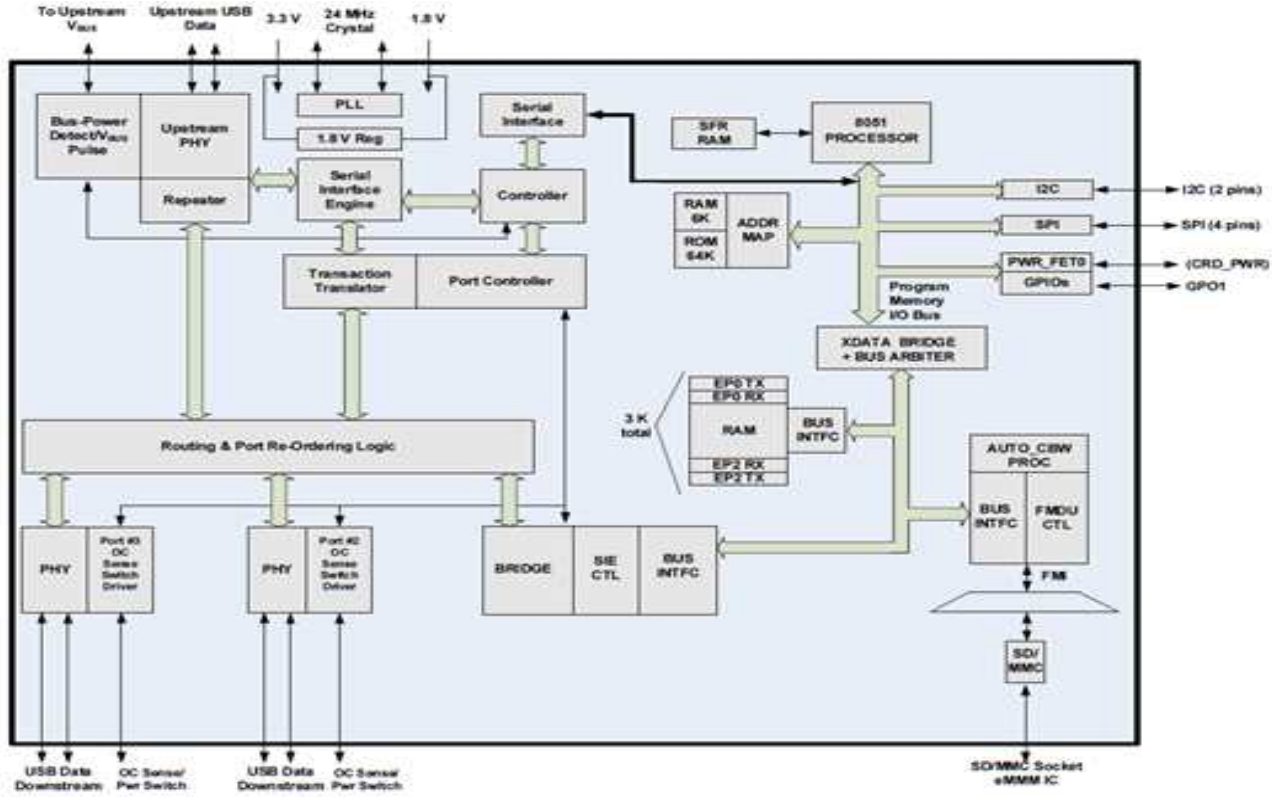


Fig. 1. USB2642 Block Diagram

3.1.2 Inter-block interface specification

Fig. 2 shows the devices matched to each interface of the USB2642 in the entire block diagram of the inter-block interface specification. The US B2642 has its own USB, SPI, and SD interfaces, and uses SDI and SPI with GPIO. Using these, SD is used as a Micro SD port, and it is matched with Micro SD using a Micro SD connector. and it was matched with BLE CC2540 using USB.

It is a device that is matched to each interface of CC2540 of wireless

communication matching part. The CC2540 has its own BLE, USB, SPI and UART interfaces. It implements the UART interface as a monitor port and matches with Flash using SPI. BLE is capable of Bluetooth communication in the 2.4GHz band.

The Power section shows the Power Block used on the current board. The power supply receives an external USB 5V, and then generates 3.3V and 3.3V using the LDO. 3.3V is supplied to USB2642 and CC2540 respectively[4].

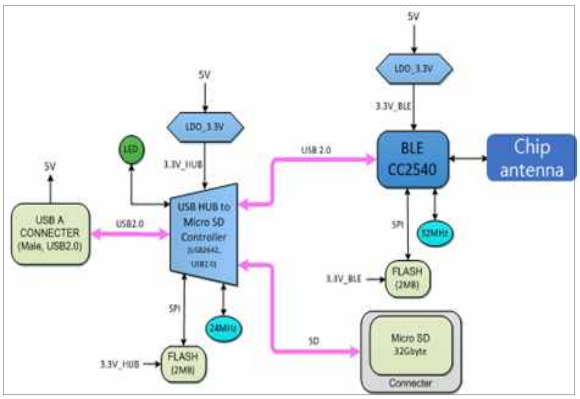


Fig. 2. Whole block diagram

3.1.3. Interface design between internal functions

Fig. 3 shows the SPI provided to the SPI Flash among the interfaces of the USB2642. This is used to change the settings of the USB2642 chip such as serial number and product.

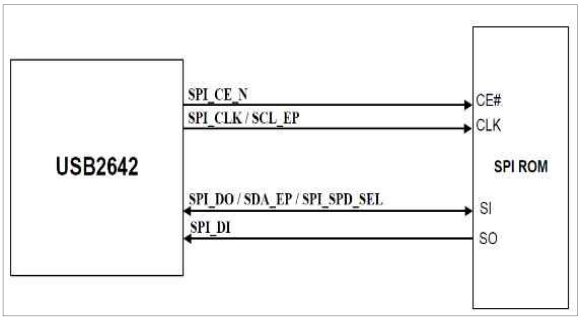


Fig. 3. SPI Block

The UART interface is a block of the CC2540's UART interface and is used for debugging. It is also used on PC via USB2642 HUB. Bluetooth Interface The Bluetooth Interface is configured using RF provided in the CC2540 Bluetooth and matches the calibration circuitry and antenna.

The frequency uses the 2.4 GHz band and the Micro SD interface is configured using the SD interface provided by USB2642 and matches the Micro SD connector[5,6].

3.2. Development of Bluetooth cipher module software

3.2.1 GAP

GAP stands for Generic Access Profile, which controls advertising and connections in Bluetooth. The core concept of the GAP is Central and Peripheral devices. Peripheral devices are primarily small, low-power devices that are designed to operate in conjunction with more resource-rich Central devices with limited resources. Heart Rate Monitor, and BLE proximity sensor tag. A Central device is a device that has enough resources, such as a phone or tablet, and resources such as memory.

3.2.2 ADVERTISING AND SCAN RESPONSE DATA

When advertising using GAP, you can include Advertising Data Payload and Scan Response Payload. The two are separate and contain up to 31 bytes of data. However, while the Advertising Data Payload is mandatory, the Scan Response Payload is optional. Advertising Data Payload is the data that is continuously transmitted from the peripheral device for the Central device to recognize. Scan Response Payload is optionally implemented as defined in the central device to require additional information such as the device name.

Fig. 4 shows how the advertising process works. First, the peripheral device has a specific advertising interval, and transmits an advertising packet for each period.

The longer the cycle, the lower the power consumption, but the slower the response at the Central unit. If you are interested in Scan Response Data at the receiving device (central device), you can send additional requests and peripheral responds with the data here[6,7].

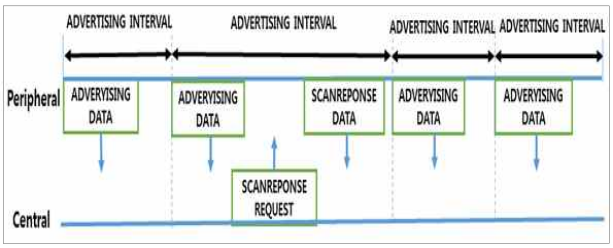


Fig. 4. Advertising course

3.2.3 BROADCASTING, BEACON

Peripheral devices can advertise their presence to nearby central devices at low cost by advertising as little as 31 bytes of data. In BLE this is called Broadcasting. The beacon is the only peripheral device that plays only the advertising role. Apple's iBeacon defines custom payload content for advertising packets to be written in a specific format. Once Central and Peripheral devices are connected, advertising is terminated and not scanned from external devices. Now, the GATT service and characteristics are used to communicate in both directions.

3.3. S/W structure

The GATT based operation structure used in BLE is based on Profile, Service, and Characteristic. Fig. (5) below shows the vertical structure of BLE operation structure[8].

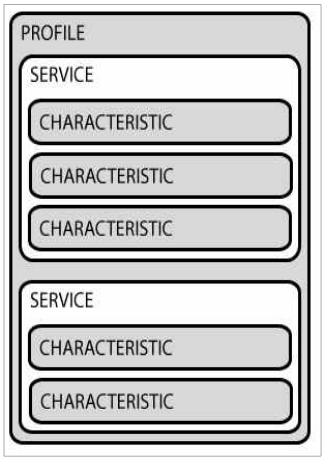


Fig. 5. BLE operation structure diagram

3.3.1 PROFILE

The profile does not actually exist in the BLE peripheral. It is a bundle of predefined services created by the Bluetooth SIG (Bluetooth Standard Development Group) or peripheral designers. For example, the Heart Rate Profile (HRP) is a combination of the Heart Rate Service (mandatory) and the Device Information Service (optional), which is defined as the Heart Rate Profile.

3.3.2 SERVICE

A service divides data into logical units and contains one or more data units called characteristics. Each service has a 16-bit (for officially adopted BLE Services) or 128-bit (for custom services) identifier called UUID. A list of official services established by the standard group can be found in [Links].

Checking Heart Rate Service shows that 16-bit UUID - 0x180D is used. This service has three characteristics (Heart Rate Measurement, Body Sensor Location, and Heart Rate Control Point), and only Heart Rate Measurement is required.

3.3.3 CHARACTERISTIC

In the GATT-based operation structure, the

lowest unit contains only one data item. If the X, Y, and Z axis values are paired like an acceleration sensor, the array of associated values is also considered as one data. If the phone displays the desired peripheral in the scan result, the peripheral device terminates advertising when the two devices are connected, and Central acts as the GATT client and connects to the GATT server.

Android, and iOS framework, it runs the GATT client and notifies the app when various events such as data reception, connection status change occur. First, it receives GATT information and Service information of the connected device and confirms it as Service UUID information, and extracts data to be actually processed by receiving Characteristic information(UUID) value.

3.4. SFMS module operation structure

Fig. 6 shows the operation flowchart of the SFMS module, performs basic H/W initialization, and waits for ID and Password to use the module. At this time, if it is normally requested from the terminal, it confirms the ID and password held by the module and transmits OK/NOK to help user control access of the application program[9].

Also, if a key for encryption/decryption is requested in the terminal in the encryption/decryption process, the encryption/decryption is performed by providing the generated key value in the module. Meanwhile, a plurality of cryptographic keys are secured, a random index is created, and a related function is implemented so that a random cryptographic key is always provided to the user[10].

For the internal security of the cloud and the terminal, the Bluetooth based cryptographic module (SFMS module) is interlocked and the application SW developed SW that can be used for Windows, Android, IoS, MaC. When the application SW is operated as a whole, the BLE interface is basically linked and the connection is normally performed. Then, input ID / PWD in the login window, and pass OK/NOK to the module[11,12].

If you need encryption according to your needs, there are automatic encryption and manual encryption. In case of automatic encryption, we developed the function to perform encryption automatically by moving the file to the automatic encryption directory, and to encrypt by using Shell Script in case of manual encryption[13].

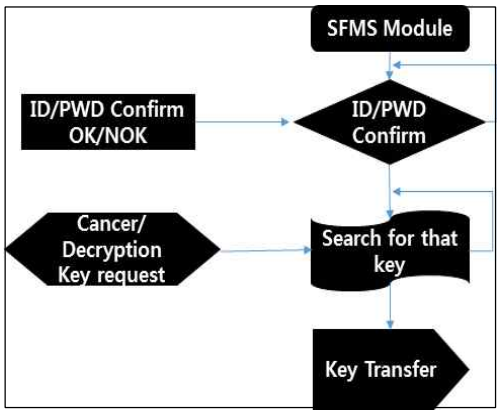


Fig. 6. SFMS module operation flowchart

4. Experiment result

Fig. 7 shows that the SW that operates on the SFMS module is basically interfaced with four terminals and classified into Windows programs, Android app programs, iPhone app programs, and MAC programs.

We used the ARIA-CBS algorithm distributed by KISA for the unification of the algorithms and tested the mutual exchange of the encryption and decryption interworking for each terminal for the compatibility test.

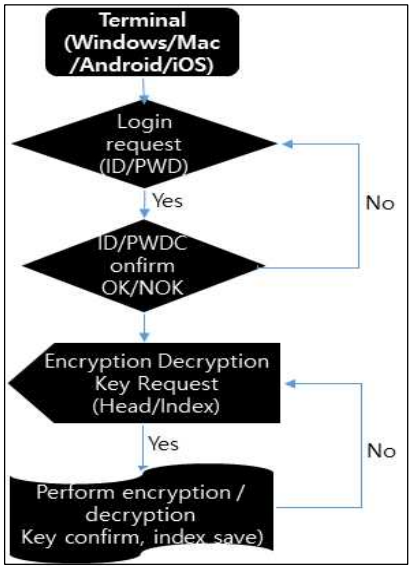


Fig. 7. SFMS OS Operation Flowchart

Table 2 confirms the results of SFMS 'Development of secure security system based on media in a cloud environment', and the evaluation results of module authentication time, key reception time, and encryption / decryption rate were evaluated appropriately.

Table 2. SFMS Test result

Test Items	Development Goals	Test result	Remarks
Module authentication time	Within 10 seconds	fitness	Windows OS, Android, Mac OS, iOS OS: Operating System
Key reception time	Within 5 seconds	fitness	
Cancellation speed	5 Mbps or higher	fitness	

※ 2018 TTA Tested Certified Test Scores

4.1. Windows OS development contents

When you execute the icon, the login screen appears. Enter the ID and password and click the login button. If the ID/password is matched, the login is performed. If the error occurs, the related function is developed so that the login cannot be performed.

I developed the related function to change the password by pressing the password change after checking the ID, password, new password and new password. After changing the password, you must unplug the SFMS module and re-install it.

Windows can encrypt/decrypt files using shell script by right clicking on the file after selecting the file and developed the function to perform file encryption/decryption function by selecting it when the menu is shown as below. Encrypted files are appended with Sec at the end of the extension.

4.2. Android OS

On the Android, menu and file management, file addition, etc. are diagrammed. When the guidance screens 1~4 are passed, the guidance screen is displayed on the 5th, but there is a function of not watching anymore. If checked, only the guide screens 1 to 4 will be displayed when the application is executed from the next time. This is the cloud personal storage interface setup screen. Clouds available are Google Drive, One Drive, and Drop Box.

To activate, select the desired cloud and follow the instructions to login. When you turn off the active cloud, you can turn it off by touching the activated cloud once in the personal storage link setting.

4.3. MacBook OS development contents

When you execute the icon, the login screen appears. Enter the ID and password and click the login button. If the ID/password is matched, the login is performed. If the error occurs, the related function is developed so that the login cannot be performed. When you log in for the first time, Bluetooth is not registered. Once Bluetooth is registered on your MacBook, you will not be asked for a Pin connection from the next login. MacBook

can encrypt/decrypt files using Shell Script by right clicking on a file and develop related functions to perform file encryption/decryption by selecting it when a menu is displayed as shown below. Encrypted files are appended with Sec at the end of the extension.

4.4. iPhone OS development contents

When you click My Drive on the main screen, it is moved to encryption folder. In the encryption folder, it is possible to encrypt by selecting TXT, photo, video file and so on. When you encrypt a file, the encrypted file is stored in the encrypted folder as shown in the figure below. The encrypted file can be selected and executed immediately. This is the cloud personal storage interface setup screen. Clouds available are Google Drive, One Drive, and Drop Box.

When the drop box is linked to the cloud, the files in the encrypted folder are automatically linked to the cloud and the encrypted txt file in the encrypted folder is linked. If you click the download button linked to the cloud, it will be downloaded to the encryption folder.

5. Conclusion

It protects information about important data inside computer and terminal and protects information about cloud internal data to fundamentally block outflow by hacking. Development of Bluetooth-based cryptographic module, application SW program development (Windows, iPhone, Android, MacBook) was developed and applied.

The Bluetooth-based information protection module has been developed to be able to interoperate with various terminal environments, and there is no information protection module that is interlocked with such various terminals worldwide for the first time in the world.

The terminal internal encryption/decryption key is determined at the time when the file is encrypted. Since the key value is separately provided for each file, the related function is developed so that the hacking itself is not possible. In addition, we developed H/W to use 32G mobile memory and USB power for light weight in order to ensure maximum convenience from the viewpoint of users.

PCs, smart phones, tablets, and cloud service in the face of social problems such as corporate existence, personal mental harm and suffering, and national security leak, personal and corporate information leaks caused by hacking, and information leakage can be prepared in advance, and it is possible to protect personal, social and national information, and solve social problems of hacking and information leakage.

In the future, it is necessary to develop a key management method that secures higher safety than existing methods, and to develop software and hardware-based encryption/ decryption methods that do not degrade computational efficiency. It is anticipated that more transparent management solutions should be developed at the user level. Therefore, cloud and media-based secure file management security system is suitable for government policy and future prospects.

REFERENCES

[1] G. Heiser, K. Elphinstone, I. Kuz, G. Klein & S. M. Petters. (2007). Towards Trustworthy Computing Systems: Taking Microkernels to the Next Level. *Operating Systems Review, 41(3),* 3-11.

[2] H. Huh & J. Lee. (2009). A Study on

Development of H8 MCU IDB(Integrated development board) for Embedded Education. *J. of the Korea Institute of Electronic Communication Sciences, 4(1),* 51-57.

[3] H. Lee & J. Oh. (2017). Design and Implementation of a Small Server Room Environment Monitoring System by Using the Arduino. *J. of the Korea Institute of Electronic Communication Sciences, 12(2),* 386-387.

[4] K. Kim, C. By on, C. Lim & S. Han. (2008). Design of Electrostatic Monitoring System. *The J. of the korea Institute of Maritime Information & Communication Sciences, 12(11),* 2069-2076.

[5] K. Kim, D. Wang & S. Han. (2017). Home Security System Based on IoT. *J. of the Korea Institute of Electronic Communication Sciences, 12(1),* 147-154

[6] D. Ryu & T. Choi. (2016). Development of Open IoT platform based on Open Source Hardware & Cloud Service. *J. of the Korea Institute of Electronic Communication Sciences, 11(5),* 485-490.

[7] H. Xu & C. Kim. (2017). Design and Implementation of a Smart Home Cloud Control System Using Bridge based on IoT. *J. of the Korea Institute of Electronic Communication Sciences, 12(5)* 866-869

[8] K Yoo & D. Ko. (2012). Study on the Performance Test Technique of Open SW-based Cloud computing. *J. Korean Institute of Information Technology, 10(7),* 185-19

[9] Y. Oh & S. Lee. (2014). IoT and the open source development platform. *J. of the Korean Institute of Information Scientists and Engineers, 32(6),* 25-30.

[10] C. Ryu. (2014). Context Inference and Sensor Data Classification of Big Data Stream Environment. *J. of The Korea Institute of Electronic Communication Sciences, 9(10),* 1079-1085.

[11] K. Nam. (2014). A Study on the Office Management Service Platform based on M2M/IoT. *J. of the Korea Institute of Electronic Communication Sciences, 9(12),* 1405-1413.

[12] D. Lee, D. Bae, S. You, J. Chae, Y. Lee & H. Yang. (2011). An Analysis on the Security of Secure Keypads for Smartphone. *Review of Korea Institute of Information Security and Cryptograph (KIISC), 21(7),* 30-37.

[13] J. Saidov, B. Kim, J. Lee & G. Lee. (2017). Hardware Interlocking Security System with Secure Key Update Mechanisms In IoT Environments. *J. of the Korea Institute of Electronic Communication Sciences, 12(4),* 671-678.

김 희 철(Kim Hee Chul) [정회원]

- 1982년 6월~1985년 12월 : 육군통신장교 중위전역
- 1990년 8월 : 조선대학교 일반대학원 컴퓨터공학과(공학석사)
- 2003년 2월 : 조선대학교 일반대학원 컴퓨터공학과(공학박사)
- 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
- E-Mail : jaziri@daum.net