The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 18, No. 5, pp.17-23, Oct. 31, 2018. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2018.18.5.17
JIIBC 2018-5-3

사물인식과 비콘을 활용한 모바일 내부정보 유출방지 시스템

Leakage Prevention System of Mobile Data using Object Recognition and Beacon

채건희, 최성민, 설지환, 이재흥*

Geonhui Chae, Seongmin Choi, Jihwan Seol, Jaeheung Lee*

요 약 모바일 기술의 급격한 발전으로 업무 간 모바일 기기 사용이 증가하였고, 이로 인한 보안사고의 가능성 역시 높아지고 있다. 사진을 통한 내부정보 유출이 가장 대표적인데, 이를 막기 위한 기존 방법들은 사생활을 침해하거나 정보 유출 목적이 아닌 다른 용도의 사진도 찍을 수 없도록 해 사용자의 불편을 야기하는 단점이 있다. 본 논문에서는 사물인식과 비콘을 활용하여 사진을 통한 내부정보 유출을 방지하는 시스템을 설계 및 구현한다. 구현 시스템은 심층학습을 기반으로 한 사물인식을 통해 사진을 검사하여 보안 정책 위반 여부를 확인한다. 또한 비콘을 통해 모바일 기기의 위치를 파악하여 그에 맞는 규칙을 적용함으로써 위치에 따른 유연한 정책 적용을 가능하게 한다. 관리자용 웹 애플리케이션을 통해 장소별로 사진 촬영에 대한 규칙을 설정할 수 있도록 하였으며, 사용자가 사진을 찍자마자 해당 위치에 적합한 규칙을 적용해 보안 정책에 어긋나는 사진을 자동으로 검출한다.

Abstract The rapid development of mobile technology has increased the use of mobile devices, and the possibility of security incidents is also increasing. The leakage of information through photos is the most representative. Previous methods for preventing this are disadvantageous in that they can not take pictures for other purposes. In this paper, we design and implement a system to prevent information leakage through photos using object recognition and beacon. The system inspects pictures through object recognition based on deep learning and verifies whether security policies are violated. In addition, the location of the mobile device is identified through the beacon and the appropriate rules are applied. Web applications for administrator allow you to set rules for taking photos by location. As soon as a user takes a photo, they apply appropriate rules to the location to automatically detect photos that do not conform to security policies.

Key Words : Object Recognition, Beacon, Deep Learning, Data Leakage Prevention, BYOD

Ⅰ. 서 론

최근 모바일 기술이 급격히 발전하면서 기존 PC에서만 가능했던 대부분의 업무를 모바일 기기에서도 처리할 수 있게 되었다. 이러한 흐름에 맞춰 기업은 개인의 모바일 기기를 직장 업무 내에 활용하도록 하는 BYOD(Bring

*정회원, 대전대학교 정보보안학과
접수일자 : 2018년 8월 14일, 수정완료 : 2018년 9월 13일
게재확정일자 : 2018년 10월 5일

Received: 14 August, 2018 / Revised: 13 September, 2018 / Accepted: 5 October, 2018
*Corresponding Author: leejh@dju.kr
Department of Computer & Information Security, Daejeon University, Korea

Your Own Device) 정책을 추진하고 있다[1]. 이를 통해 업무의 효율성을 높이고, 비용을 절감할 수 있어 이 정책은 널리 확산되고 있는 추세이다.

하지만 모바일 기기의 특성으로 인한 다양한 보안사고의 가능성 또한 높아졌다[2]. 대표적인 것 중 하나가 사진을 통한 내부정보 유출이다. 기업에서는 이를 막기 위해 내부 인력을 대상으로 무작위 사진 검사를 실시하기도 하고, MDM(Mobile Device Management)[3, 4]이나 보안 스티커를 통해 회사 안에서 사진을 찍을 수 없도록 규제하고 있다. 하지만 이러한 방식은 사생활을 침해하거나 정보 유출 목적이 아닌 다른 용도의 사진도 찍을 수 없도록 하여 사용자들의 불만을 사고 있다.

본 논문에서는 사물인식과 비콘을 활용하여 사진을 통한 내부정보 유출을 방지하는 시스템을 설계 및 구현한다. 본 논문에서 구현한 시스템은 심층학습(Deep Learning)[5, 6]을 기반으로 한 사물인식을 통해 사람이 아닌 기계가 사진을 검사하여 보안 정책을 위반하였는지 여부를 판단하도록 한다. 또한 기업의 촬영 관련 보안 정책은 기업의 성향 및 내부 부서의 특성에 따라 장소마다 다를 수 있다. 본 논문에서 구현한 시스템은 비콘을 통해 모바일 기기의 위치를 파악하여 그에 맞는 규칙을 적용하도록 함으로써 위치에 따른 유연한 정책 적용을 가능하게 한다. 관리자용 웹 애플리케이션을 통해 장소별로 사진 촬영에 대한 규칙을 설정할 수 있도록 하였으며, 사용자가 사진을 찍자마자 해당 위치에 적합한 규칙을 적용해 보안 정책에 어긋나는 사진을 자동으로 검출한다. 따라서 사용자가 출장 또는 부서 이동으로 익숙하지 않은 곳에 가서 생길 수 있는 보안 정책 미숙으로 인한 사고도 미연에 방지할 수 있다.

본 논문은 다음과 같이 구성된다. 2장에서는 관련 연구로 심층학습을 통한 사물인식과 비콘에 대해 간단히 살펴보고, 3장에서 시스템의 동작 과정 및 전체 구조에 대해 설명한다. 4장에서 구현 결과를 확인하며, 마지막으로 5장에서 결론을 맺는다.

II. 관련 연구

1. 심층학습을 통한 사물인식

인공 뉴런은 신경계의 뉴런을 모사하여 고안한 간단한 연산 기능만을 가진 처리기로 입력된 신호와 가중치를 각각 곱한 결과를 모두 더한 다음, 활성함수를 취한 값을 출력한다. 인공신경망[7]은 생물학의 신경망에서 영감을 얻어 개발한 학습 알고리즘으로 인공 뉴런이 학습을 통해 결합 세기를 변화시켜 문제를 해결할 수 있도록 한 비선형 모델이다. 가장 기본적인 인공신경망 알고리즘인 다층인공신경망의 경우 입력층, 은닉층, 출력층으로 구성되며 입력층과 출력층 사이 다수의 은닉층이 존재하는 것을 심층신경망이라고 한다. 심층학습은 이러한 심층신경망을 모델로 입력 데이터의 특징을 도출하는 기계학습 알고리즘으로써 높은 수준의 추상화를 통하여 이미지 속 사물인식을 가능하게 한다[5, 8]. 사물인식은 이미지 속에서 특정 사물의 존재 여부를 판단하는 것으로 심층학습을 통하여 수많은 이미지들을 학습시켜 도출된 학습 데이터를 바탕으로 사물인식을 진행하는 방법을 가장 많이 사용한다[6].

2. 비콘

블루투스 4.0에 새롭게 추가된 BLE(Bluetooth Low Energy)는 기존보다 빠르진 않지만 소비전력을 크게 낮춘 것이 특징이다. 이러한 BLE 프로토콜 기반 근거리 무선통신 장치인 비콘은 인식 거리 약 70m, 측위 오차 5cm 이내, 저전력 등의 장점으로 IoT 인프라를 구축하는데 있어 많이 사용되고 있다[9]. NFC와 같이 4~5cm로 근접할 필요도 없으며 GPS보다 정확한 위치 인식이 가능하다는 장점으로 모바일 기기와 연동하여 여러 장소에서 사용자의 위치에 따른 다양한 서비스를 제공하는 것이 가능하다.

III. 내부정보 유출방지 시스템 설계

1. 시스템 동작 과정

전체 시스템 동작 과정은 그림 1과 같고, 주요 작업 흐름은 그림 2와 같다. 각 장소마다 비콘이 있어 고유 UUID(Universal Unique ID) 값을 주기적으로 브로드캐스트한다. 모바일 기기에 설치된 사용자 애플리케이션은 해당 지역의 비콘이 전송한 UUID 값을 받아(1), 서버에 보낸다(2). 서버는 받은 UUID 값을 바탕으로 해당 지역의 규칙 목록을 보낸다(3). 규칙 목록에는 촬영금지 사물, 거리 제한 범위, 비콘의 설치 장소 정보가 들어있으며, 이는 관리자용 웹 애플리케이션을 통해 설정할 수 있다. 사

용자는 애플리케이션 구동 후 로그인 과정을 통하여 사용자 인증을 받고 모바일 기기에 설치된 외부 애플리케이션을 선택하여 사진을 촬영한다(4). 촬영된 사진은 그림 3과 같이 스트림 암호화를 적용하여 사용자가 볼 수 없도록 하고, 모바일 기기 내에서 사물인식을 수행하거나(5-1), 아니면 서버에 이미지 정보를 보내 사물인식을 수행한다(5-2). 사물인식이 끝나면 결과를 받아(6), 규칙 목록과 비교하여 서버에 알림을 보내거나 사진을 삭제 또는 복호화한다(7).

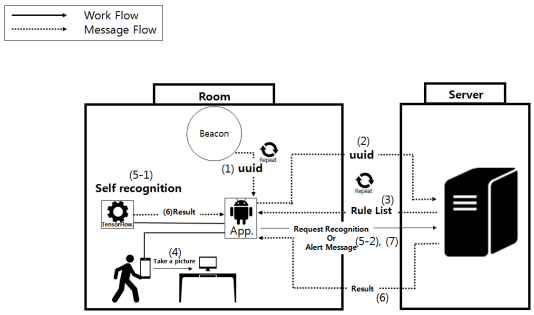


그림 1. 시스템 동작 과정
Fig. 1. System operation process

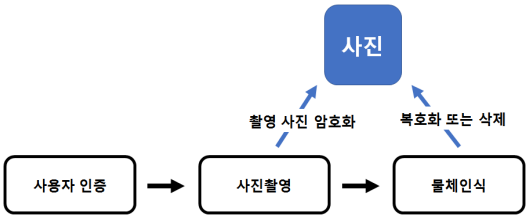


그림 2. 주요 작업 흐름
Fig. 2. Main workflow

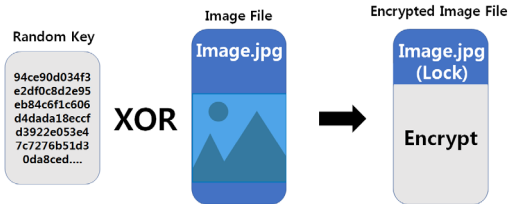


그림 3. 이미지 파일 암호화
Fig. 3. Image file encryption

2. 시스템 구조

전체 시스템 구조는 아래 그림 4와 같다. LoginActivity는 애플리케이션 구동 초기에 동작하며 주변 비콘을 바인딩하고 UUID 값을 서버에 보내어 규칙 목록을 받는다. 또한 이 클래스는 로그인 기능을 내장하고 있으며 입력된 아이디와 패스워드를 서버로 전송하여 사용자 인증을 수행한다. 인증이 성공적으로 수행되면 CameraLuncher Activity가 시작된다. 이 클래스는 모바일 기기에 설치된 외부 카메라 애플리케이션을 불러오며 사용자는 원하는 카메라 애플리케이션으로 사진 촬영을 할 수 있다. 또한 외부 카메라 애플리케이션을 이용하여 사진 촬영 시 CameraLuncherActivity는 촬영된 사진을 즉각 암호화하고 RecognizeImageService를 동작시켜 암호화된 사진에 대하여 사물인식을 요청한다. RecognizeImageService는 규칙에 따라 서버 사물인식, 혹은 자가 사물인식을 수행하며 결과를 LoginActivity에서 수집한 규칙 목록과 비교하여 암호화된 이미지 파일을 삭제, 혹은 복호화시킨다. 사물인식 결과 사진에 규칙 목록에 포함된 사물이 촬영되었을 경우 서버의 PostAlertMessage에 알림을 보내어 관리자가 해당 정보를 볼 수 있도록 한다. 또한 서버에서 RuleMaker를 통하여 각 장소별로 설치된 비콘의 UUID를 등록한 뒤 각 위치에 알맞은 규칙 목록을 작성할 수 있으며, 규칙 목록에는 촬영금지항목 및 추가 옵션들을 설정할 수 있도록 하였다.

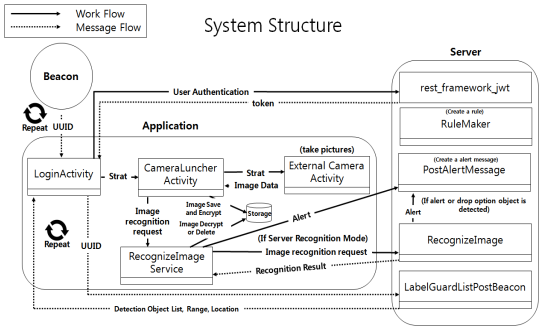


그림 4. 시스템 구조
Fig. 4. System structure

3. 사용자 애플리케이션 내부 동작 과정

그림 5는 사용자 애플리케이션의 사진 촬영부터 사물인식까지의 동작 과정을 보여준다. CameraLuncher Activity에서 외부 카메라 애플리케이션을 불러와 사진 촬영을 하면 촬영된 사진의 이미지 파일이 생성되고 촬영된 이미지를 무작위 난수를 통하여 암호화시킨다. 이후 암호화된 사진의 경로와, 암호화에 사용된 키값(무작위 난수)을 RecognizeImageService에 보내어 사물인식을 진행한다. RecognizeImageService는 이미지 경로와

키값을 활용하여 해당 암호화된 이미지로부터 비트맵 데이터를 추출한다. RecognizeImageService는 추출된 비트맵 정보를 통하여 사물인식을 진행한다. RecognizeImageService가 수행하는 과정은 스레드풀 방식을 통해 하나씩 순차적으로 진행되며 인식 스레드는 FIFO 방식으로 순서대로 사물인식을 진행한다. 이와 같은 방식을 통하여 사용자는 연속된 촬영 혹은 사진 촬영 이외의 다른 작업이 가능하며 사물인식이 완료되지 않은 사진은 암호화되어 있는 상태로 존재한다. 또한 이러한 과정을 통하여 사용자는 이 시스템에 종속된 카메라 액티비티를 사용하지 않고 원하는 카메라 애플리케이션을 사용할 수 있도록 하여 익숙한 카메라 환경에서 사진 촬영이 가능하도록 하였다.

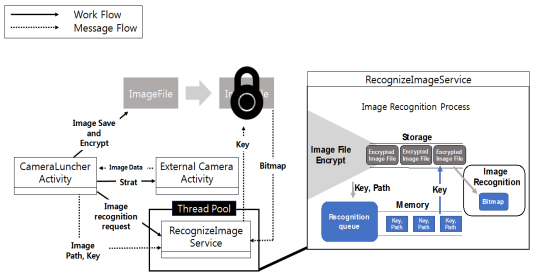


그림 5. 사용자 애플리케이션 내부 동작 과정
Fig. 5. User application internal operation process

Ⅳ. 내부정보 유출방지 시스템 구현

본 논문에서 구현한 모바일 내부정보 유출방지 시스템의 개발 및 실행 환경은 표 1과 같다. 전체 시스템은 사진 촬영 및 사물인식을 위한 모바일 애플리케이션과 관리자가 실시간으로 장소에 따른 규칙을 설정하고 알림을 받기 위해 사용하는 웹 애플리케이션, 장소를 인식하기 위한 비콘, 사물인식과 장소에 따른 규칙 목록을 반환하는 서버 애플리케이션으로 구성된다.

그림 6은 관리자용 웹 애플리케이션의 규칙 설정 화면을 보여준다. 그림 6의 비콘 등록 버튼을 누르면 그림 7의 왼쪽 다이얼로그를 통해 비콘 정보를 설정할 수 있다. 그 후 그림 6의 장소 내 규칙 설정 버튼을 눌러서 그림 7의 오른쪽 다이얼로그를 통해 장소별 촬영 금지 목록 및 세부 옵션을 설정하면 된다. 제안 시스템 구현 시 세부 옵션으로 Alert와 Drop을 구현하였으며 Alert를 선택하면 사용자에게 경고 메시지와 함께 그림 8의 관리자 알림판에 노란색 알림이 가게 되고, Drop을 선택하면 사진은 자동 삭제되고 관리자 알림판에 붉은색 알림이 가도록 하였다. 그림 9는 사용자 로그 기록 페이지로 실시간으로 사용자의 시스템 사용 여부를 확인할 수 있다.

표 1. 시스템 개발 및 실행 환경
Table 1. System development and execution environment

구성 요소	개발 환경	실행 환경
Android App.	Android Studio (Java 1.7)	Android Lolipop 5.0 or higher
Web App.	Cloud9 (HTML5, CSS, Javascript)	Chrome 63.0 or higher IE 11 or higher Safari 10 or higher
Beacon		reco beacon(iBeacon)
Server	Javascript, Python Angular.js 1.6.7 bootstrap 3.3.7 TensorFlow 1.8.0	Django Framework

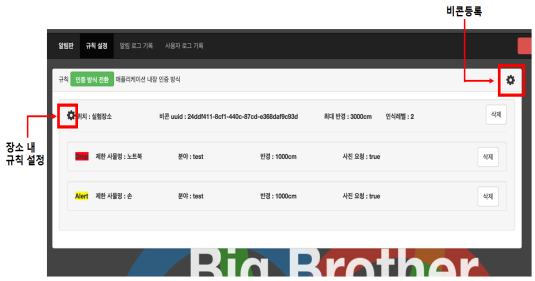


그림 6. 관리자용 웹 애플리케이션 (규칙 설정)
Fig. 6. Web application for administrators (rule setting)

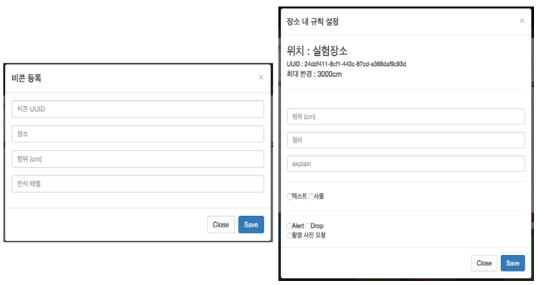


그림 7. 비콘 설정 및 장소 내 규칙 설정 다이얼로그
Fig. 7. Beacon configuration and location rule setting dialog

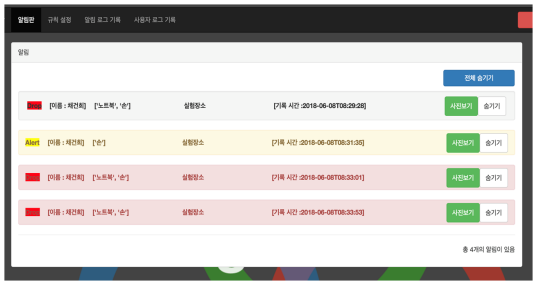


그림 8. 관리자용 웹 애플리케이션 (알림판)
Fig. 8. Web application for administrators (notice board)

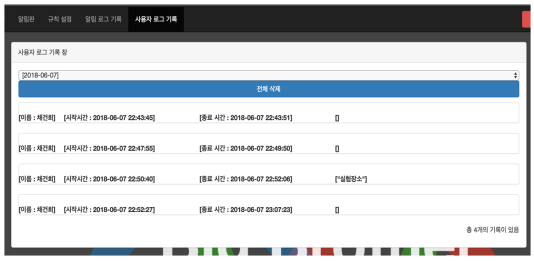


그림 9. 관리자용 웹 애플리케이션 (사용자 로그)
Fig. 9. Web application for administrators (user log)

그림 10, 그림 11, 그림 12는 사용자 애플리케이션 화면을 보여준다. 테스트를 위해 손이 촬영되면 서버에 알림 메시지를 보내고(Alert 옵션), 노트북이 촬영되면 해당 사진을 삭제하도록(Drop 옵션) 규칙을 설정하였다. 사용자는 그림 10의 1번 로그인 화면을 통해 인증을 받고, 2번 화면을 통해 카메라 애플리케이션을 선택할 수 있다. 그림 11의 1번 사진을 통해 확인할 수 있다시피, 사진 촬영 시 적용될 수 있는 규칙 목록을 시각적으로 바로 볼 수 있도록 하였으며, 노트북이 촬영될 경우 사진을 삭제하고(2번 사진), 손이 촬영되었을 때 이를 인식하는 것(3번 사진)을 알 수 있다. 그림 12의 1번 사진은 노트북을 촬영한 사진과 손을 촬영한 사진이 저장소에 저장된 상태로 사물인식이 완료될 때까지 암호화되어 있음을 알 수 있다. 사물 인식 결과 노트북이 발견되면 알림과 함께 사진을 삭제하고(2번 사진), 손이 감지되면 알림만 발생시키는 것을 볼 수 있다(3번 사진).

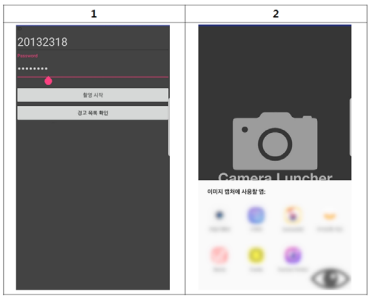


그림 10. 사용자 애플리케이션 (1. 로그인, 2. 카메라 선택)
Fig. 10. User application (1. login, 2. camera selection)

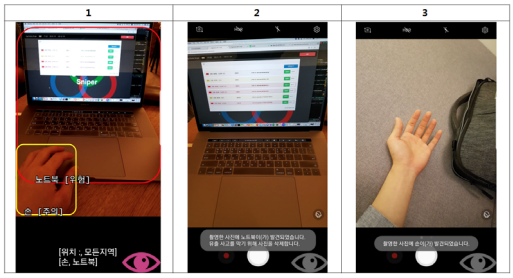


그림 11. 사용자 애플리케이션 (사진)
Fig. 11. User application (photo)

그림 12. 사용자 애플리케이션 (사진 저장소)
Fig. 12. User application (photo storage)

V. 결 론

본 논문에서는 사물인식과 비콘을 활용하여 사진을 통한 내부정보 유출을 방지하는 시스템을 제안하고 구현하였다. 제안 시스템은 비콘을 통해 장소마다 그에 맞는 사진 촬영 보안 정책을 적용할 수 있도록 하였으며, 관리자용 웹 애플리케이션을 통해 실시간으로 정책을 설정할 수 있도록 하였다. 사용자가 사진을 찍자마자 정책 위반 여부를 확인하여 삭제할 수 있도록 하여 사진을 통한 내부정보 유출을 사전에 방지하고, 보안 정책 미숙으로 인

한 사고 역시 막을 수 있다.

제안 시스템에서 사진을 검사하기 위해 사용한 사물 인식 모델은 시스템 종속적이지 않아 추후 사물인식 기술이 발전함에 따라 인식률 및 인식 속도가 증가하면 이를 시스템에 쉽게 반영할 수 있다.

References

[1] Yookyoung Park, Bongsun Kim, Sungmin Rue, “The Technologies to Protect the Confidential Information from BYOD Trend,” Korea Institute of Information Technology Magazine, Vol. 13, No. 1, pp. 49-54, June 2015.

[2] Seonho Shin, Jieun Shin, Hyunbong Kim, Jiman Jeong, JinWoo Son, MyungKeun Yoon, “Enterprise-Data Leakage Prevention in BYOD,” Korean Journal of Industry Security, Vol. 5, No. 2, pp. 7-44, Dec. 2015.

[3] Kanghyun Lee, Dooshik Yoon, “MDM's Effective Approach to Mobile Security,” REVIEW OF KIISC, Vol. 23, No. 2, pp. 29-34, Apr. 2013.

[4] Junho Lim, Kangseok Kim, Hongjin Yeh, “A Method for Minimizing Security Threats for Mobile Applications in MDM System,” Journal of KIISE : Computing Practices and Letters, Vol. 19, No. 12, pp. 693-697, Dec. 2013.

[5] Jürgen Schmidhuber, “Deep learning in neural networks: An overview,” Neural Networks, Vol. 61, pp. 85-117, Jan. 2015.
DOI: 10.1016/j.neunet.2014.09.003

[6] Y. Bengio, A. Courville, P. Vincent, “Representation Learning: A Review and New Perspectives,” IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 35, No. 8, pp. 1798-1828, Aug. 2013.
DOI: 10.1109/TPAMI.2013.50

[7] Y. Jung, D. Kim, C. Hong, J. Lee, H. Kwon, “The study to measure of the BTX concentration using ANN,” Journal of the Korea Academia-Industrial cooperation Society, Vol. 5, No .1, pp. 1-6, March 2004.

[8] Hyuncheol Park, Sangwoong Lee, “CNN-facilitated Color and Character Recognition in Practical Applications,” The Journal of Korean Institute of Next Generation Computing, Vol. 12, No. 6, pp. 104-115, Dec. 2016.

[9] Hyungseo Kang, Insoo Koo, “Beacon Node Based Localization Algorithm Using Received Signal Strength(RSS) and Path Loss Calibration for Wireless Sensor Networks,” The Journal of the Institute of Internet, Broadcasting and Communication, Vol. 11, No. 1, pp. 15-22, Feb. 2011.

저자 소개

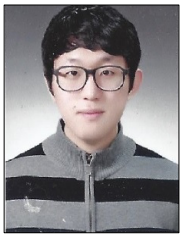
채 건 희(준회원)

• 2013년 3월 ~ 현재 : 대전대학교 정보보안학과 학사 재학
<주관심분야 : 보안 시스템 개발>

최 성 민(준회원)

• 2013년 3월 ~ 현재 : 대전대학교 정보보안학과 학사 재학
<주관심분야 : 네트워크 보안, 리버스 엔지니어링>

설 지 환(준회원)



• 2013년 3월 ~ 현재 : 대전대학교 정보보안학과 학사 재학
<주관심분야 : 안드로이드 개발 및 보안, 클라우드 보안>

이 재 홍(정회원)

- 2001년 2월 : 서울대학교 컴퓨터공학부 졸업
- 2003년 2월 : 서울대학교 전기, 컴퓨터공학부 석사
- 2013년 2월 : 서울대학교 전기, 컴퓨터공학부 박사
- 2016년 3월 ~ 현재 : 대전대학교 정보보안학과 조교수

<주관심분야 : 암호학, 정보보호, 시스템 보안, 무선 보안>

※ 이 논문은 2016학년도 대전대학교 교내학술연구비 지원에 의해 연구되었음.