JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 23, No. 8: 1018~1023, Aug. 2019

LINK 블록체인을 적용한 차량용 블랙박스 시스템

안규황[1] · 원태연[1] · 박상민[1] · 장경배[1] · 서화정[2*]

Vehicle black box system with LINK blockchain

Kyuhwang An[1] · Taeyeon Won[1] · Sangmin Park[1] · Kyoungbae Jang[1] · Hwajeong Seo[2*]

[1]Graduate Student, Department of IT Engineering, Hansung University, Seoul 02876, Korea
[2*]Assistant Professor, Department of IT Engineering, Hansung University, Seoul 02876, Korea

요 약

2010년도를 기점으로 차량용 블랙박스는 많은 사람들에게 보급되었음에도 불구하고 차량 사고 현장 기록물이 존재 하지 않거나 가해자가 고의적으로 영상 데이터를 삭제할 경우 피해자가 속출한다. 블록체인의 가장 큰 장점은 데이터 분산 저장으로 데이터 수정 및 삭제가 불가능하다는 점이며, 가장 큰 단점은 민감한 데이터 역시 분산 저장 된다는 점이다. 본 논문은 해당 장점을 이용해 블랙박스에 블록체인을 도입하여 공유 된 영상 데이터로 사고를 입증하며, 블록체인과 private 서버를 연동하여 기존에 블록체인에 저장되는 민감 정보를 private 서버에 저장하여 블록체인의 단점인 개인정보유출 문제를 해결하고자 한다. 또한 LINK 블록체인과 private 서버를 연동하는 코드(깃허브)와 데모 영상(유튜브)을 본 논문에 첨부하였다.

ABSTRACT

Since 2010, vehicle black boxes have become popular with many people, if there is no record of the vehicle accident scene, or if the offender deliberately deletes the image data, the victim succeeds. The biggest advantage of blockchain is that it is impossible to modify and delete data by data distribution storage. The biggest disadvantage is that sensitive data is also distributed. In this paper, we propose a blockchain method for the black box by using the advantage of shared block data and we intend to solve the problem of personal information leakage which is a disadvantage of blockchain by storing sensitive information stored in a blockchain in a private server by LINK blockchain with a private server. We also attached code(Github) and demonstration video(Youtube) linking LINK blockchain with the private server in this paper.

키워드 : 분산 처리, 블랙박스, LINK 블록체인, 차량 사고, 인증

Key word : Distributed Computing, Black Box, LINK Blockchain, Vehicle Accident, Authentication

Received 30 January 2019, **Revised** 6 February 2019, **Accepted** 3 March 2019

*** Corresponding Author** Hwajeong Seo(E-mail:hwajeong@hansung.ac.kr, Tel:+82-2-760-8033)
Assistant Professor, Department of IT Engineering, Hansung University, Seoul 02876, Korea

Open Access http://doi.org/10.6109/jkiice.2019.23.8.1018 print ISSN: 2234-4772 online ISSN: 2288-4165

ⓒThis is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(http://creativecommons.org/li-censes/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright Ⓒ The Korea Institute of Information and Communication Engineering.

Ⅰ. 서 론

2010년도를 기점으로 차량용 블랙박스 시장이 급증하기 시작하였다. 현재는 운전자의 93.2%가 차량용 블랙박스가 필요[1]하다는데 공감하고 있으며, 그에 걸맞게 많은 운전자들이 차량용 블랙박스를 사용하고 있다. 그림 1은 최근 블랙박스 시장과 보급률을 나타내는 그래프이다.

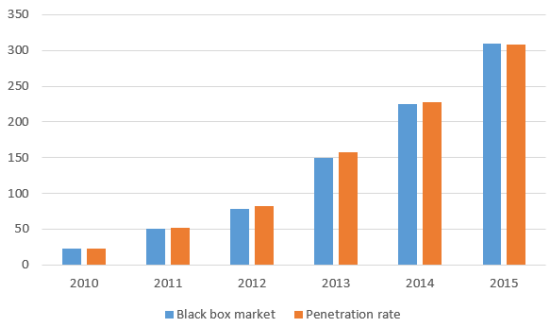


Fig. 1 Black Box Market Status

그러나 우리는 일상생활을 하면서 교통사고 목격자를 찾는 플랜카드들을 흔히 마주친 경험이 있다. 이러한 이유는 첫 번째로 차량과 사람의 사고가 발생한 경우 일반적으로 차량의 운전자의 과실이 크다고 생각되면 블랙박스의 영상을 공개하지 않는다. 두 번째로 현대인들은 본인이 관련 된 사고가 아닌 이상 남의 일에 개입하고 싶어 하지 않는 가치관이 상당하기 때문이다.

블록체인을 블랙박스에 적용하여 차량사고가 났을 경우 블록체인 참여자들이 원하는 블랙영상을 제공받고 그것을 제공해준 대상자에게 보상을 지급해주는 형태의 시스템을 제안하고자 한다. 또한 여기서 사용하는 블록체인은 라인에서 블록체인 서비스를 위해 사용하는 LINK 블록체인 이용하여 시스템을 구축하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구 동향을 살펴볼 것이며, 3장에서는 본론에 해당하는 제안 기법을 설명한다. 4장에서는 기존 시스템과 제안 기법 상의 비교를 통한 평가를 할 것이며, 5장에서 끝을 맺도록 하겠다.

Ⅱ. 관련 연구 동향

블록체인이 대중에 화두로 떠오름에 따라 다양한 분야에 적용하고자 하는 시도가 이루어진다. 따라서 블록체인이 무엇인지 알아본 이후 어떤 분야에 블록체인을 적용하고 있는지 알아보고자 한다.

2.1. Blockchain Technology

블록체인 기술은 사토시 나카모토(Satoshi Nakamoto)[2]가 비트코인(Bitcoin)이라는 암호 화폐(crypto-currency)를 고안하다 탄생한 기술로 현재 우리가 사용하는 화폐를 보면, 중앙은행에서 모든 입·출금 장부를 기록하는 방식으로 이루어져 있다. 이렇게 되면 제 3자인 중앙은행에 내 화폐를 관리 및 감독을 해주기 때문에 일정 수수료를 지불해야한다. 또한 제 3자인 중앙은행이 내가 사용하는 화폐의 흐름을 마음대로 관찰할 수 있어 중앙은행 측에서 개인정보보호가 제대로 이루어진다고 100% 확신하여도 사용하는 소비자들의 입장에서는 불안한 것이 사실이다. 사토시 나카모토는 금전적 거래를 함에 있어 중개인인 제 3자를 없애고 소비자와 판매자 간에 P2P(Peer to Peer) 방식으로 진행되길 원했다. 블록체인 기술은 기존에 나의 모든 정보를 저장하는 중앙 서버를 없애는 대신 거래에 참여한 모든 사람의 컴퓨터에 모두의 기록을 저장하는 방식으로 제 3자인 중앙 서버를 없앴다. 이렇게 되었을 경우의 이점은 보다 투명한 거래를 할 수 있고 중개인이 없음으로써 중개 비용을 절감할 수 있다. 중앙 서버가 존재할 때는 데이터 보안에 대한 것은 따로 걱정하지 않아도 되었었다. 그러나 각자의 컴퓨터에 데이터를 저장하는 블록체인에서는 내 데이터가 위변조 되지 않을까 걱정이 되기 마련이다. 이 걱정을 해결하기 위해 사토시 나카모토는 해시 값(hash value)을 사용하였다. 전송할 때 각 header 블록 안에 고유의 해시 값과 전송 시간이 저장되게 되고 전송 시간을 이용하여 바로 이전에 전송한 블록과 전송하려는 블록이 해시 값에 의해 체인과 같이 그림 2처럼 연결되게 된다. 전송하려는 블록 header에 이전 해시 값이 저장되고, 바로 이전 블록에는 전전 해시 값이 저장된다. 이런 방식으로 최초의 블록까지 모든 블록이 연결되기 때문에 보통 수십 만개를 넘는 블록으로 구성되는 블록체인을 악의적 의도로 위변조하려 하면 모든 블록의 해시 값을 수정 해줘야하기 때문에 전문가들은 위변조가 불가능한 아주

안전한 암호화 방식이라고 말한다.

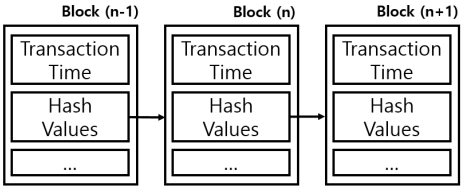


Fig. 2 Block connected by hash values

2.2. 블록체인을 활용한 자전거 관리 시스템 구축[3]

일본의 경우 자전거를 자동차와 같은 취급을 하여 구매를 하면 자전거를 등록[4]을 해야지만 사용할 수 있다. 그러나 대한민국의 경우 자전거 등록제가 법적 의무가 아니기 때문에 자전거를 구입하면 바로 사용할 수 있다. 사용자 측면에서 자전거를 등록하지 않고 바로 사용할 수 있기 때문에 번거롭지 않아 더 좋을 것 같지만, 실상은 그렇지 않다. 첫 번째로 자전거가 관리가 되고 있지 않기 때문에 해당 자전거가 도난 제품인지 알 방법이 없다. 두 번째로 과거에 큰 사고가 났었는지 어떤 부품에는 이상이 있는지 알 수 있는 방법이 없다. 이러한 문제점을 블록체인을 활용하여 자전거 관리 시스템을 만들어 해결하고자 한다.

해당 논문에서 제안하는 시스템은 웹을 기반으로 돌아가는 시스템으로 블록체인을 데이터베이스로 사용하여 사용자들의 자전거 차대번호를 등록하고, 해당 시스템에서 사용자들의 자전거 차대번호를 조회하여 실제 주인이 맞는지 확인할 수 있다. 또한 교통사고가 발생해 자전거를 수리해야할 경우 블록체인 상에 어떠한 문제점이 발생하여 어딜 수리하고 어떠한 부품으로 갈았는지도 모두 기입하며 블록체인 내부 구조는 그림 3과 같다.

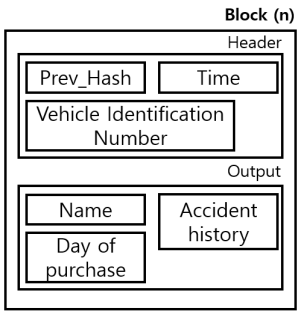


Fig. 3 Blockchain structure of bicycle VIN blockchain

Ⅲ. 제안 기법

본 논문에서 사용하는 블록체인은 라인에서 사용하는 LINK 블록체인을 사용하여 블랙박스 시스템을 구현하고자 한다. LINK 블록체인 블랙박스 시스템을 구현하는데 있어, 라즈베리파이를 이용하여 블랙박스 역할을 구현하였으며 리눅스에 LINK 블록체인 서버를 구축하였다. 각각의 시스템 환경은 표1, 2와 같다.

Table. 1 Private server system environment

OS	Raspbian
Database	MySQL
Hardware	Raspberry pi 3 B
Development Language	Python 3

Table. 2 LINK blockchain system environment

OS	Ubuntu 18.04
LevelDB	1.18-5
Libsecp256k	.
RabbitMQ	3.7.9
Python	3.0
tbears	.

적용 시나리오는 다음과 같다. LINK 블록체인 블랙박스를 장착한 자동차가 도심을 활보할 때, 해당 블랙박스는 10분 단위로 동영상을 녹화한다. 녹화한 동영상에 대한 정보인 '위도, 경도, 사용자 ID, 녹화 시간'에 대한 정보는 sha256 함수(sha256(latitude | longitude | user_ID | transaction_time))를 통해 암호화 된다. 암호화 된 값은 동영상에 대한 제목으로 정의된다. Sha256에 대한 입력값은 LINK 블록체인 상에 저장되며, 동영상은 private 서버에 저장되게 된다. 이때 주의할 점은 한 곳에 모든 동영상이 저장되는 것이 아닌, 개발자가 정의한 위도·경도 값에 해당하는 table에 저장되게 된다. 이는 그림 4와 같다.

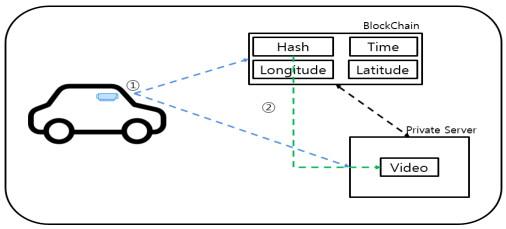


Fig. 4 The architecture of how to work

그림 5는 사고가 발생했을 경우에 대해 증명하는 절차이다. 왼쪽 상단에 폭발 표시된 지역에서 차량 사고가 발생했다고 가정했을 때 직접적으로 사고에 연관된 자동차 외에 해당 지역을 보고 있는 차량 역시 블랙박스를 통해 사고에 대한 영상 정보를 가지고 있다. 해당 영상을 획득하고 싶은 사용자는 사고 발생 지점 DB table에 접근하여 동영상을 획득할 수 있다.

Fig. 5 How to verify car accident

LINK 블록체인으로 구현된 블랙박스를 장착한 차량이 도심을 활보할 때 일어나는 현상은 다음과 같다. 먼저 LINK 블록체인 블랙박스는 10분 단위로 동영상을 녹화한다. 녹화한 영상과 해당 영상에 대한 정보(위도, 경도, 사용자 id, transaction 시간)가 블록체인에 전송되게 된다. 이때 녹화된 영상의 경우 블록체인에 저장되는 것이 아닌 별도의 private 서버에 저장된다.

영상을 블록체인이 아닌 private 서버에 저장하는 이유는 블록체인의 경우 블록체인에 저장된 데이터는 누구나 열람이 가능하다. 이때 차량용 블랙박스는 사용자의 위치 정보와 사용자가 어떠한 일을 하였는지 어디로 이동하였는지 알려주는 역할을 하게 된다. 이는 개인정보에 아주 치명적이다.

유럽 연합에 의하면 2018년 5월부터 개인정보보호법(GDPR)[5]을 설립하였으며, 위법을 어길 경우 최대 전 세계 매출액의 4%를 유럽 연합에 과징금을 제출해야한다. 이때 주의해야 할 점은 단순히 유럽에서 발생하는 개인정보 유출에만 해당하는 것이 아닌 유럽에 거주하지 않는 유럽인의 개인 정보가 유출되어도 동일한 법에 처벌된다. 이에 따라 기업들은 개인 정보 보호에 각별히 신경써야하는 실정이다.

블록체인의 가장 큰 단점은 누구나 데이터에 접근 할 수 있다는 점이다. 블록체인에 참여한 사용자는 내 정보뿐만 아니라 다른 사람들의 정보를 모두 저장하게 된다. 만약 블록체인에 저장되는 정보들이 주민등록번호와 같이 민감한 정보일 경우, 내 정보가 다른 사용자의 컴퓨터에 저장되기 때문에 이는 아주 위험한 행위이다. 본 논문에서는 블록체인의 단점을 극복하기 위해 블록체인에 저장할 수 없는 민감한 데이터는 그림 4에서 설명한 바와 같이 sha256 함수(sha256(latitude | longitude | user_ID | transaction_time))를 통해 암호화된 값을 private 서버에 저장하는 방식을 제안하고자 한다.

먼저 LINK 블록체인을 사용하려면 tbears[6]라는 플랫폼을 설치하는 행위가 선행되어야 한다. tbears는 블록체인 사설 에뮬레이터를 실행시킬 수 있도록 도와주는 역할을 하며, 설치 명령어는 그림 6과 같다.

```
# Install levelDB
$ sudo apt-get install libleveldb1 libleveldb-dev

# Install libSecp256k
$ sudo apt-get install libsecp256k1-dev

# install RabbitMQ and start service
$ sudo apt-get install rabbitmq-server

# Create a working directory
$ mkdir work
$ cd work

# Setup the python virtualenv development environment
$ virtualenv -p python3 .
$ source bin/activate

# Install LINK SDK
(work) $ pip install tbears
```

Fig. 6 Command line to download tbears

tbears 설치가 완료되면, (work) $ tbears start 명령을 활용하여 구동시킬 수 있다. tbears를 구동하고 나면, LINK 블록체인을 사용할 수 있게 된다. 하지만 LINK 블록체인에 들어갈 내부 데이터 값을 사용자에 맞게 변경하기 위해선, work 폴더에 있는 call-hello.json 파일을 사용자의 목적에 맞게 수정해야한다. call-hello.json 파일의 구성은 그림 7과 같다. 해당 json 파일을 수정하고 나면 사용 준비가 완료된다.

```
{
    "jsonrpc": "2.0",
    "method": "icx_call",
    "params": {
        "to": "{your LINK Contract address}",
        "dataType": "call",
        "data": {
            "method": "hello",
            "params": {
            }
        }
    },
    "id": 1
}
```

Fig. 7 JSON structure of call-hello.json

Private 서버 측에서는 LINK 블록체인과 정보를 주고받을 수 있는 서버 측 역할이 필요하다. 해당 역할은 python을 이용하여 그림 8과 같이 구현하였다. 블랙박스(라즈베리파이)는 녹화한 영상을 sha256을 통해 hash 값으로 변환한다. 해당 hash 값을 동영상의 제목으로 설정한다. 카메라 녹화 영상 10분 경과 시 위에서 암호화한 해시 키를 이용하여 private 서버에 전송함과 동시에 LINK 블록체인 내부에 기록하는 값인 '위도, 경도, 사용자 id, transaction 시간' 값을 트랜잭션한다.

```
class connectServer(threading.Thread):
    def __init__(self,addr,savePeriod):
        threading.Thread.__init__(self)
        self.addr = addr
        self.savePeriod= savePeriod
    def run(self):
        global camera
        first=True
        while True:
            if first == False:
                preFileName=fileName

(1)         fileName=time.strftime("%y%m%d_%H:%M:%S",time.localtime())
            fileName=sha256.encrypt_string(fileName)
            camera.updateFileName(str(fileName))
            if first==True:
                first=False
                time.sleep(self.savePeriod)
                continue

(2)         client.requestMessage(self.addr, str(preFileName))#request foward to server
            file = {'file':open('localRepository/'+preFileName+'.avi','rb')}
            client.requestUpload(self.addr, file)#request foward to server
            time.sleep(self.savePeriod)
```

Fig. 8 A private server send information code to LINK Blockchain

블랙박스(라즈베리파이)에서 전송한 정보와 암호화된 값을 이용하여 private 서버에 저장한 결과는 그림 9와 같으며, 왼쪽 위에 터미널을 보면 라즈베리파이에서 전달 된 해시 값(드래그 된 영역)과 동영상의 제목이 일치함을 확인할 수 있다.

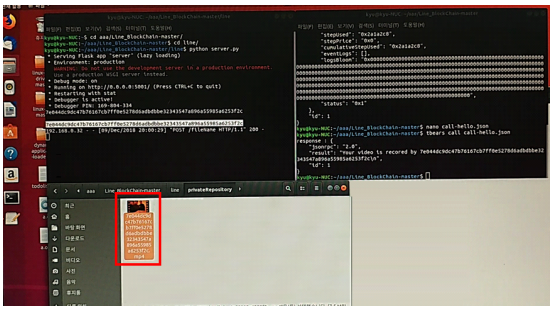


Fig. 9 A result of video on private server

Ⅳ. 비교 분석

본 장에서는 기존에 사용자들이 사용하는 블랙박스 시스템과 LINK 블록체인을 적용한 블랙박스 시스템 간의 성능에 대해서 비교 분석해 보겠다.

기존 블랙박스의 경우 녹화하는 동영상을 남들과 공유하는 것이 아닌 본인만 소유한다. 만약 사람의 왕래가 없는 도로에서 사고가 발생할 경우 운전자는 악의적으로 블랙박스를 비공개할 것이다. 이렇게 되면 피해를 입은 사용자는 어디에 호소할 곳도 없이 피해를 직면하게 된다.

그러나 LINK 블록체인을 활용한 블랙박스는 녹화한 동영상을 본인만 소유하는 것이 아닌 남들과 공유하는 플랫폼이다. 또한 사용자가 직접 블록체인에 동영상을 업로드 하는 방식이 아닌 10분 간격에 자동으로 업로드 한다. 따라서 해당 플랫폼을 사용하는 사용자와 사고가 날 경우 피해자는 증거 영상에 대해 걱정할 필요가 없다. 따라서 기존 블랙박스보다 활용도가 높다고 판단할 수 있다.

또한 LINK 블록체인을 활용한 블랙박스의 경우 다방면으로 활용할 수 있는 가치가 높다. 예를 들어 도심을 활보한 영상이 저장된 동영상 데이터에 컴퓨터 비전 기술과 인공지능을 접목하여 미아 찾기 혹은 강력범 찾기와 같은 사회적으로 활용할 수 있다.

Ⅴ. 결 론

블록체인의 가장 큰 장점은 한번 값이 저장되면 삭제

및 수정이 불가능하며, 가장 큰 단점은 민감한 정보를 다른 사람에게 공개하게 될 수 있다는 점이다. 만약 LINK 블록체인을 적용한 블랙박스 시스템을 많은 사람들이 사용한다면, 블록체인의 장점을 이용하여 도로 위에서 발생하는 사고들에 대해 대부분의 영상 데이터를 확보할 수 있으며, 운전자의 잘못으로 발생한 사고를 LINK 블록체인을 통해 해결할 수 있다. 또한 블록체인의 단점인 민감 데이터 공유 방지는 private 서버를 통해 해결할 수 있다.

해당 논문에서 구현한 결과는 유튜브[7]에 업로드 했으며, 구현한 코드는 깃허브[8]에 공개되어있다.

본 논문에서 제안하는 방식은 private 서버를 이용한 permissioned blockchain으로 접근을 통제하고 있다. 향후 연구 계획으로 permissionless blockchain에 대해 알아보고자 한다. 또한 속성기반 암호와의 결합을 통해 보다 나은 보안성 강화도 가능할 것으로 예상된다 [9].

ACKNOWLEDGEMENT

This research was partly supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2019-2014-1-00743) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation) and this research was partly supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2017R1C1B5075742).

References

[1] Money Today: 500 Billion Car Black Box Market [Internet]. Available : http://news.mt.co.kr/mtview.php?no=2013102815173610911&outlink=1&ref=http%3A%2F%2Fm.blog.daum.net

[2] Bitcoin. Bitcoin: A Peer-to-Peer Electronic Cash System [Internet]. Available: https://bitcoin.org/bitcoin.pdf.

[3] K. H. An, H. J. Seo, 2018, "Building bicycle management system using Blockchain," Journal of the Korea Institute of Information and Communication Engineering, Vol. 22, No. 8, pp. 1139~1145. Aug. 2018.

[4] Steemit: Bicycle registration system in Japan (Internet) Available: https://steemit.com/kr/@pdiwin/6659rp

[5] GDPR: European Privacy Protection Act GDPR Guide (Internet). Available: https://www.privacy.go.kr/gdpr

[6] Github: How to use tbeas (Internet). Available: https://github.com/icon-project/t-bears

[7] Youtube: Implementation video (Internet). Available: https://youtu.be/WW87_LKmjnI

[8] Github: source code (Internet). Available: https://github.com/kyu-h/Line_BlockChain

[9] Y. T. Kim, H. Kim, H. Jo, D. Lee, "Secure Messenger System using Attribute Based Encryption," Journal of Security Engineering, Vol.12, No.5 pp.469-486, Aug. 2015.

안규황(Kyu-hwang An)

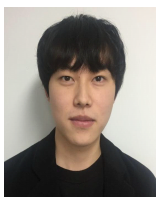
2018년 2월: 한성대학교 IT응용시스템공학과 공학 학사
2018년 3월~현재: 한성대학교 IT융합공학과 석사과정
※ 관심분야 : 암호구현, IoT 보안, 블록체인

원태연(Tae-Yeon Won)

2018년 2월: 한성대학교 정보시스템공학과 공학 학사
2018년 3월~현재: 한성대학교 컴퓨터공학과 석사과정
※ 관심분야 : 딥러닝, 컴퓨터비전, 임베디드

박상민(Sang-Min Park)

2018년 2월: 한성대학교 IT응용시스템공학과 공학 학사
2018년 3월~현재: 한성대학교 컴퓨터공학과 석사과정
※ 관심분야 : 딥러닝, 강화학습



장경배(Kyoung-Bae Jang)

2019년 2월: 한성대학교 IT응용시스템공학과 공학 학사
2019년 3월~현재: 한성대학교 IT융합공학과 석사과정
※ 관심분야 : IoT, 정보보안

서화정(Hwa-jeong Seo)

2010년 2월 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월 부산대학교 컴퓨터공학과 석사 졸업
2012년 3월~2016년 1월: 부산대학교 컴퓨터공학과 박사 졸업
2016년 1월~2017년 3월: 싱가포르 과학기술청
2017년 4월~현재: 한성대학교 IT 융합공학부 조교수
※ 관심분야 : 정보보호, 암호화 구현, IoT