Journal of KIIT. Vol. 18, No. 7, pp. 51-56, Jul. 31, 2020. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2020.18.7.51

블록체인 기반 이동식 저장 장치 기록 관리 시스템

고준형*, 이규성**, 김희열***[1], 김남기***[2]

A Log Management System of Removable Storage Devices Based on Blockchain

Jun-Hyung Ko*, Gyu-Seong Lee**, Heeyoul Kim***[1], and Namgi Kim***[2]

본 논문은 2020학년도 경기대학교 대학원 연구원장학생 장학금 지원에 의하여 수행되었음. 또한, 교육부의 재원으로 한국연구재단의 지원(NRF-2017R1D1A1B04027874)을 받아 수행된 연구임.

요 약

전자 문서의 사용이 대두되면서 이동식 저장 장치의 사용이 보편화 되었다. 이로 인하여 이동식 저장 장치에 대한 보안 사고는 그 위험성이 더욱 증대되고 있다. 본 논문은 이동식 저장 장치를 통한 정보 유출을 방지하기 위한 파일의 암/복호화와 해당 정보 유출시 그 원인을 투명하게 파악할 수 있는 시스템을 제안한다. 제안하는 시스템은 블록체인을 활용한 비대칭키 방식으로 파일의 암/복호화를 수행한다. 또한, 사용자의 파일 사용/편집 기록을 블록체인에 저장하여 정보의 분산과 무결성을 확보한다. 이 시스템의 세부적인 내용으로 스마트 컨트랙트를 기반으로 하는 보안 정책 위반 대응을 제안한다. 또한, 블록체인을 통해 해당 파일에 대한 로그 수집/기록 과정을 구현한다. 그 결과 수집된 로그들의 무결성 보증을 확인한다.

Abstract

As the use of electronic documentation, the use of removable storage devices has become common. Due to this, the risk of security incidents for removable storage devices is increasing. This paper proposes a system that can encrypt & decrypt of files and transparently identify the cause of information leakage from removable storage devices. The proposed system performs the encryption and decryption of the file in public key method using the block chain. Also, user's file usage and editing logs are stored in the block chain to ensure the distribution and integrity of information. With details of the system, we propose a violation of the security policy response based on a smart contract. Also it implements a log collecting and recording process of the file through the block chain. As a result, the integrity assurance of the collected logs is confirmed.

Keywords

removable storage, log collection, block-chain, smart contract

* 경기대학교 컴퓨터과학과 석사과정
- ORCID: http://orcid.org/0000-0001-7258-9721
** 경기대학교 컴퓨터과학과 학사과정
- ORCID: http://orcid.org/0000-0001-8735-7501
*** 경기대학교 컴퓨터과학과 교수([2]교신저자)
- ORCID[1]: http://orcid.org/0000-0001-6341-580X
- ORCID[2]: http://orcid.org/0000-0002-0077-6576

· Received: Apr. 16, 2020, Revised: Jul. 20, 2020, Accepted: Jul. 23, 2020
· Corresponding Author: Namgi Kim
Division of Computer Science and Engineering, Kyonggi University, 154-42, Gwanggyosan-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do, Korea
Tel.: +82-31-249-9662, Email: ngkim@kyonggi.ac.kr

Ⅰ. 서 론

과거부터 컴퓨터를 통한 전자문서 처리의 보편화가 진행되었다. 전자문서 처리의 용이성은 해당 문서의 경중을 막론하고 적용되었으며 그 결과 중요한 기밀 내용에 대해서도 전자문서화가 진행되었다. 이러한 추세에 따라 중요한 자료들을 무단으로 이동식 저장 장치에 복사하여 반출하는 보안사고 및 중요한 PC에 이동식 저장 장치를 통한 바이러스 공격 등 보안을 위협하는 공격이 증가하였다. 이를 막기 위하여 이동식 저장 장치들을 관리하고 보안성을 확립하기 위해 여러 방법이 제시되었다. 그 방법들로는 DLP(Data Loss Prevention)와 DRM(Digital Rights Management)등이 사용되고 있다.

소프트웨어를 통한 이동식 저장 장치 관리[1]는 보안성 확립을 위한 여러 방법들 중 하나이다. 그 영역은 단순 저장장치 복구부터 시작하여 장치 사용 범위 제한까지 다양한 범위가 존재한다. 하지만, 소프트웨어 기반 관리 방법은 이동식 저장 장치 사용 기록을 완전 삭제와 같은 방법으로 변조 및 무결성이 훼손될 수 있다. 본 논문에서는 이러한 문제점을 극복하기 위하여 기존에 사용 중인 소프트웨어 관리 방식에 블록체인 기술을 도입하여 보다 신뢰할 수 있는 시스템을 제안한다. 본 논문에서는 블록체인이 적용된 이동식 저장 장치 관리 기법 중 로그들이 블록체인에 저장되는 과정을 구현하며 이를 통해 해당 로그들의 보증된 무결성을 제시한다.

Ⅱ. 관련 연구

퍼블릭 블록체인은 개방형 블록체인 네트워크로 누구나 블록체인 네트워크에 참가하여 트랜잭션 생성하고 블록을 채굴하여 트랜잭션을 원장에 기록할 수 있으며 원장의 내용을 누구나 확인할 수 있다. 하지만, 누구나 참여할 수 있고, 블록을 생성할 수 있는 특성 때문에 이에 대한 악의적인 사용자가 발생할 수 있다. 악의적 사용자가 정보 변조를 시키는 비잔틴 장군 문제[2]처럼 신뢰할 수 없는 네트워크의 노드들로부터의 합의를 끌어내기 위해 비트코인과 이더리움은 POW(Proof Of Work)[3] 합의 알고리즘을 사용한다. POW 알고리즘에도 문제점은 존재하기에 이를 보완하기 위한 POS(Proof Of Stake)[4], DPOS(Delegated POS)[5] 합의 알고리즘이 등장하였다.

하이퍼레저 패브릭(Hyperledger fabric)은 프라이빗(Private) 블록체인으로써 참여 권한이 부여된 참여자들로 네트워크가 이루어지게 된다. 하이퍼레저 페브릭은 참여자들 사이에서도 권한을 나누어서 원장의 데이터를 읽는데 제한을 둘 수 있다. 또한 블록을 생성하는 노드가 정해져 있으며 비잔티움 장애 허용[6]을 만족시키는 합의 알고리즘으로 Practical byzantine fault tolerance를 적용할 수 있다. 본 논문에서는 폐쇄망을 목표로 하고 있기에 참여자를 제한하고, TLS 인증서, 등록 인증서에 대해 fabric-CA 인증기관을 통해 보안을 지원하는 하이퍼레저 패브릭[7]을 기반으로 시스템을 제안한다.

사내 문서보안 및 문서 유출 방지/탐지 솔루션들 중 내부자를 대상으로 하는 성격이 가장 큰 방안은 파일 보안 시스템이 해당된다. 파일 보안 시스템들에는 DLP와 DRM[8][9]이 존재한다. DLP는 파일/문서를 PC 외 다른 외부 매체에 저장하는 등 외부 반출이 진행될 때 그것을 경고하거나 막는 역할을 한다. DRM은 디지털 컨텐츠에 대하여 허가받은 사용자만이 열람/편집을 할 수 있게 하는 시스템이다.

DLP[10][11]는 세부적으로는 엔드포인트, 서버 그리고 네트워크[12]와 같이 3가지로 구분할 수 있다. 그 중 보안성이 가장 높은 것은 엔드포인트 DLP이며 해당 방식은 사용자의 PC에 에이전트를 설치하여 PC 안에서 이뤄지는 모든 흐름들을 다 추적하고 감시하는 방식이다. 에이전트는 PC를 추적/감시하고 해당 기록을 로그로서 남기게 된다.

로그는 모든 사용자 데스크톱에서 실행된 행위에 대한 기록이라고 볼 수 있다. 로그를 복구 방침의 기준으로 잡거나 장애 발생 시 오류 추적을 위해서 활용하기도 한다. 이 때문에 수집되는 로그에 대한 무결성 확보는 한층 더 중요해진다[13]. 하지만 기존 방식들은 해당 기록들을 중앙기관에서 관리/수집하지만 그것이 해당 로그의 무결성을 보장하지는 않는다. 또한, 중앙기관에서 로그를 수집/관리하게 되면서 정보의 집중이라는 취약점을 내포하게 된다.

본 논문은 앞서 서술한대로 사용자 인가/등록하는 사설망에 적용된다. 제안하는 연구는 해당 환경 내에서 자료 유출 방지용 파일 암/복호화 및 작업

로그 무결성 확보를 블록체인을 활용하여 제안한다.

III. 블록체인 기반 이동식 저장 장치 관리

3.1 개요

제안하는 블록체인 기반 이동식 저장장치 기록 관리 시스템의 구조는 그림 1과 같다. 시스템에서 사용자 PC는 블록체인 네트워크로 서로 연결되어 같은 데이터를 가진 원장을 공유한다. user1은 file.txt를 인가된 사용자만 사용할 수 있도록 하기 위해 usb1에 file.txt를 암호화하여 저장한다. usb1내의 file.txt 파일을 사용하려는 user2는 file.txt 복호화 과정을 거쳐야 사용할 수 있다. 파일을 암호화, 복호화 행위를 비롯한 저장 장치의 모든 로그는 실시간으로 트랜잭션에 담겨서 전파되며, 트랜잭션의 검증이 완료되면 블록체인의 모든 참여자는 해당 트랜잭션을 원장에 추가하게 된다.

3.2 네트워크 참여자의 허가 및 정책 관리

하이퍼레저 패브릭은 허가받은 참여자만 네트워크에 참가할 수 있기 때문에 필연적으로 해당 허가/인가 작업을 수행할 수 있는 기관이 필요하다. CA를 통해서 참여자들의 X.509 형태의 인증서를 발급하여 디지털 신원을 인증하여 허가된 참여자인지 확인할 수 있도록 한다. 허가된 참여자는 저장 장치의 파일들에 대해 정책을 수립할 수 있다[14].

3.3 암/복호화 과정 시나리오

네트워크 참여자들은 사용자 등록 시점에 등급별 파일에 접근할 수 있는 등급 권한을 부여받는다. 저장된 파일들은 여러 등급의 개인키를 보유하고 있으며 공개키는 원장에 저장되어 있다. 등록된 사용자가 이동식 저장 장치를 사용할 때의 시나리오는 다음과 같이 진행된다.

① 1등급 권한의 user1은 usb에 1등급 권한의 참여자들만 file.txt를 열어볼 수 있도록 암호화하기 위해 1등급 공개키를 원장에 요청한다.
② 원장은 user1의 네트워크 참여자 여부 및 적정 권한 조회 후 1등급 공개키를 반환한다.
③ 반환된 공개키를 통해 file.txt를 암호화한다. 1등급 공개키로 암호화되었기 때문에 1등급 개인키가 있어야만 file.txt를 복호화하여 사용할 수 있다.
④ 암호화된 파일을 usb에 저장한다.

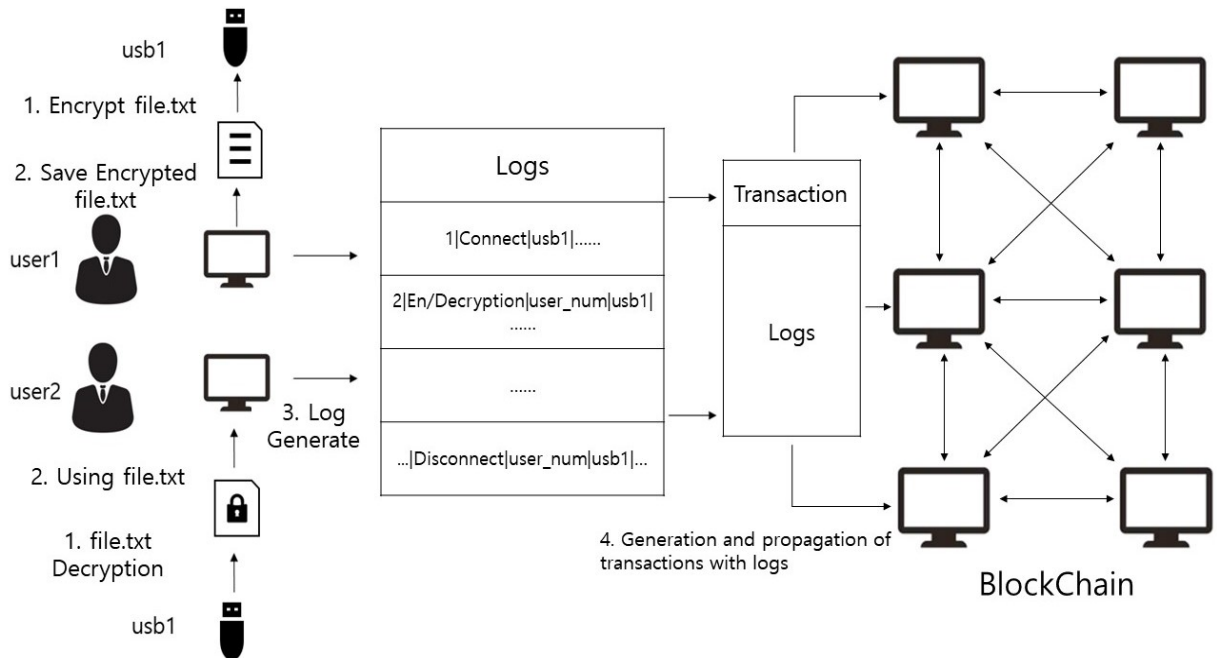

그림 1. 이동식 저장 장치 제어/감시 전체 구조
Fig. 1. Removable storage device control / monitoring overall structure

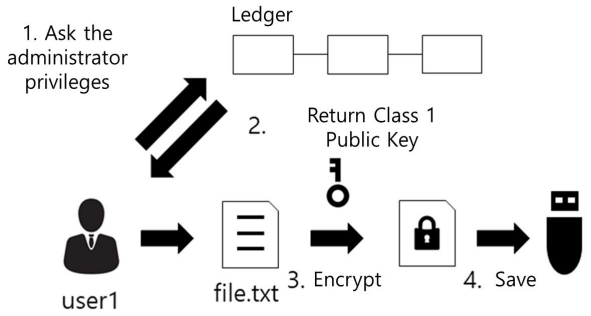

그림 2. file.txt 암호화 과정
Fig. 2. file.txt encryption process

복호화 순서는 다음과 같다.

① file.txt를 사용하려는 user2은 1등급 암호화가 걸려있는 file.txt를 usb로부터 가져온다.

② 1등급 권한인 user2는 로컬에 1등급 개인키가 저장되어 있다. 가지고 있는 1등급 개인키를 통해 file.txt를 복호화하여 file.txt를 사용할 수 있다.

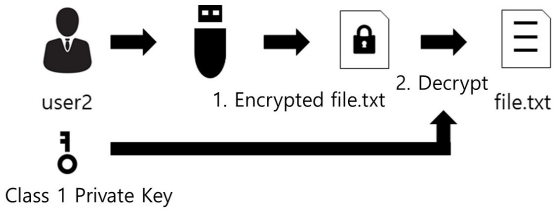

그림 3. file.txt 복호화 과정
Fig. 3. file.txt decryption process

3.4 수집되는 로그의 내용

이동식 저장 장치 사용 로그를 내용에 따라 구분하자면 ① 장치의 PC 연결 시작 정보, ② 해당 장치에 파일 복사/이동 등 편집 작업 정보, ③ 장치의 PC 연결 해제 정보로 정리할 수 있다.

이동식 저장 장치 사용 시간 로그는 해당 장치가 접속한 PC의 레지스트리 내에 기록하게 된다. 또한, 이동식 저장 장치와 PC간 이루어진 통신은 USB 버스를 모니터링 하여 해당 정보를 수집할 수 있다. 결과적으로 해당 내용들이 취합되어 이동식 저장 장치 사용 로그로서 저장된다.

이렇게 수집된 내용을 테이블 형태의 데이터로 정리 후 트랜잭션을 전송하여 블록체인에 기록하게 된다. 해당 로그를 조회하는 것을 통해 어떤 클라이언트에서 어떤 이동식 저장 장치를 활용하여 무슨 행동을 했는지 확인할 수 있다. 또한, 해당 로그가 블록체인에 기록되면서 무결성을 확보함과 동시에 정보의 분산을 달성하게 된다.

3.5 로그에 대한 처리과정

이동식 저장장치 사용 로그에 대한 처리 과정은 다음과 같다. 먼저 이동식 저장장치의 연결 확인 후 접속 시각에 대한 트랜잭션을 전송, 동시에 해당 접속에 정책 검사를 시행한다. 보안 정책에 위배되는 연결/접속은 스마트 컨트랙트를 통해 실시간으로 보안 관리자에게 경고한다. 파일의 이동/복사 기록들은 변화가 발생하는 즉시 해당 작업의 타임스탬프를 비롯한 정보들을 로그로 기록한다. 마지막으로 작업이 종료된 사용자가 이동식 저장장치를 연결 해제함과 동시에 기록되는 해제 시간을 수집한다. 이 일련의 과정들을 진행 중에 실시간으로 계속해서 트랜잭션을 수행하여 블록체인에 저장한다. 작업이 전부 완료되었을 경우 블록체인 내에는 최종적으로 작업 시작, 작업 변동 내역, 작업 종료에 관한 3가지 기록들이 순차적으로 전송/검증되며 이후 해당 내용을 조회 가능하다.

3.6 로그 블록체인 저장 시나리오

블록체인 저장 시나리오는 다음과 같다.

① user1이 usb내의 file.txt 파일을 사용한다.

② user1에 설치되어있는 에이전트 프로그램이 타임스탬프, 행위, 저장 장치의 시리얼 키 등 수행한 프로세스의 상세 로그를 그림 4와 같이 파일로 남긴다.

③ 스마트 컨트랙트가 해당 로그 파일을 읽는다.

④ user1의 정보와 모든 로그를 담은 트랜잭션을 전송하여 원장에 모든 로그가 기록되도록 한다.

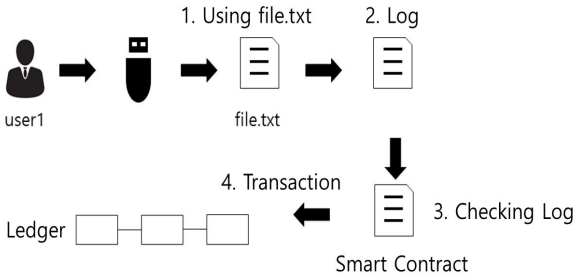

그림 4. 로그를 원장에 기록하는 과정
Fig. 4. Process of writing logs to the ledger

Ⅳ. 제안 기법에 대한 실제 구현

본 논문에서 제안하는 기능은 ① 사용자 인가 및 파일 암/복호화, ② 해당 사용자의 파일 편집/사용 기록 무결성 확보 총 두 가지이다. 이 중 사용자 인가 및 파일 암/복호화의 경우 블록체인 사용이라는 특징을 제외하면 현재 공개되어있는 여러 에이전트 프로그램에서 수행되고 있는 영역이다. 따라서 해당 영역에 대한 구현은 생략한다. 본 논문에서는 로그를 원장에 기록하는 부분인 파일 편집/사용 기록 무결성 확보 영역의 구현을 수행한다. 구현은 하이퍼레저 패브릭 v1.1.0과 Ubuntu 16.04 LTS 환경 하에서 이루어졌다.

먼저 user1이 이동식 저장장치를 사용한다고 가정해보자. user1의 PC에서 실행되고 있는 에이전트가 저장장치 연결 시작부터 연결 해제까지의 log를 csv형태의 파일로 저장한다. invoke.js를 실행하면 해당 로그파일을 읽어서 각 로그를 트랜잭션에 담아서 각 피어에 전송하게 된다. 피어들로부터 트랜잭션이 유효한지, 전자서명이 올바른지 확인한 후에 orderer에게 보내서 트랜잭션을 정렬 후 다시 배포한다. 트랜잭션 수행 후 조회해보면 그림 5에서 user1이 2019-09-25, 20:19에 Grab.g4b파일을 읽었다는 로그가 원장에 잘 기록된 것을 확인할 수 있다.


```
"user1"}},{"Key":"LOG99","Record":{"action":"파일 읽기","
desc":"JETFLASH TRANSCEND_64GB","docType":"log","fileName
":"J:\\_ISO\\e2b\\grub\\Grab.g4b","fileType":".g4b file",
"pid":"TRANSCEND_64GB (1000)","serial":"11AJFH5RBMHC3AV0"
,"timestamp":"2019-09-25 20:19","user":"DESKTOP-H1LE11A$"
,"userDesc":"","vid":"JETFLASH (8564)","wallet":"user1"}}
]
```


그림 5. 트랜잭션 조회
Fig. 5. View transaction

4.1 오프체인 단계에서의 무결성 확보

본 논문에서 제안하는 연구를 크게 2가지로 분리해서 볼 수 있다. ① 해당 작업들의 기록을 트랜잭션 수행 전 ② 트랜잭션 수행 후 블록체인에 저장. 이 중 트랜잭션 수행 후 블록체인에 저장될 경우 블록체인의 특성상 무결성이 확보된다고 할 수 있다.

블록체인에 저장되기 전 단계는 오프체인 단계이며, 해당 단계에 대한 무결성 확보는 다음과 같은 사항으로 해결할 수 있다. ① 본 논문에서 제안하는 연구는 폐쇄망 내 사용을 고려로 한 연구이다. 그로 인하여 일차적으로 사용자에 대한 선별이 이루어지며 이를 통해 어느 정도 무결성을 확보할 수 있게 된다. ② 작업을 수행할 때 기록에 변동사항이 발생하는 즉시 트랜잭션을 수행하며 이에 따라 해당 기록에 개입하기가 어려워진다. ③ 트랜잭션이 수행될 경우 해당 트랜잭션은 블록체인 트랜잭션 특성 상 무결성을 가지게 된다. 이러한 요소에 따라 기록의 트랜잭션 수행단계에서의 무결성이 확보된다.

Ⅴ. 결 론

내부망에 대한 제어/감시의 중요성은 날이 갈수록 증대되고 있다. 본 논문은 파일 유출 방지 시스템으로 이동식 저장장치 사용 로그를 수집하여 블록체인에 기록하는 방식을 제안하며 그 과정을 구현하였다. 이를 통해 정보의 분산을 수행함과 동시에 보다 향상된 무결성을 확보하게 되었다. 결과적으로 내부망에 대한 보다 효과적인 사용자 인가 및 파일 암/복호화와 파일 편집/사용 기록 무결성 확보를 할 수 있을 것으로 기대된다.

향후 연구에서는 해당 방안이 무결성을 보증함을 객관적이고 수학적인 증명을 통해 보이고, 그 로그를 활용하여 실시간 대응을 수행하는 효과적인 방안에 대하여 제시 및 연구할 계획이다.

References

[1] Michael Fabian, "Endpoint security: managing USB-based removable devices with the advent of portable applications", Proceedings of the 4th annual conference on Information security curriculum development, Kennesaw Georgia, Article No. 24, pp. 155-159, Sep. 2007.

[2] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem", ACM Transactions on Programming Languages and Systems (TOPLAS), Vol. 4, No. 3, pp. 382-401, Jul. 1982.

[3] Proof-of-Work, Explained, https://cointelegraph.com/explained/proof-of-work-explained. [accessed: Jul. 06, 2020]

[4] Proof of Stake (PoS) Definition, https://www.investopedia.com/terms/p/proof-stake-pos.asp. [accessed: Jul. 06, 2020]
[5] D.: Delegated proof-of-stake (DPOS). Bitshare whitepaper, https://www.bitshares.foundation/papers/BitSharesBlockchain.pdf. [accessed: Jul. 06, 2020]
[6] C. Miguel and L. Barbara, "Practical byzantine fault tolerance and proactive recovery", ACM Transactions on Computer Systems, Vol. 20, No. 4, pp. 398-461, Nov. 2002.
[7] Architecture of the Hyperledger Blockchain Fabric, https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf. [accessed: Jul. 06, 2020]
[8] Lakbabi, A., Orhanou, G, and Hajji, S. E, "Network Access Control Technology-Proposition to Contain New Security Challenges", International Journal of Communications, Network and System Sciences, Vol. 5, No. 8, pp. 505-512, Jan. 2012.
[9] IEEE Standard for Local and Metropolitan Area Networks-Port-Based Network Access Control, https://ieeexplore.ieee.org/document/9018454. [accessed: Jul. 06, 2020]
[10] Tobias Wuchner and Alexander Pretscher, "Data Loss Prevention Based on Data-Driven Usage Control", 2012 IEEE 23rd International Symposium on Software Reliability Engineering, Dallas, TX, USA, pp. 151-160, Nov. 2012.
[11] Simon Liu and Rick Kuhn, "Data Loss Prevention", IEEE IT Professional, Vol. 12, No. 2, pp. 10-13, Mar. 2010.
[12] Won-Jin Lee, Kee-Won Kim, Ki-Dong Bu, and Jongjung Woo, "A Study on the Adoption of NAC for Guaranteeing Reliability of u-Campus Network", The Journal of Korean Institute of Communications and Information Sciences, Vol. 7, No. 4, pp. 252-258, Aug. 2009.
[13] Log Injection-OWASP. https://www.owasp.org/index.php/Log_Injection. [accessed: Jul. 06, 2020]
[14] Maja Vukasovic, Bogdana Veselinovic, and Zarko Stanisavljevic, "A Deveolopment of a configurable system for handling X509 certificates", 2017 25th Telecommunication Forum (TELFOR), Belgrade, Serbia, pp. 1-4, Nov. 2017.

저자소개

고 준 형 (Jun-Hyung Ko)

2020년 2월 : 경기대학교 컴퓨터과학과
2020년 3월 ~ 현재 : 경기대학교 컴퓨터과학과 석사과정
관심분야 : 머신러닝, 네트워크, 통신시스템

이 규 성 (Gyu-Seong Lee)

2016년 3월 ~ 현재 : 경기대학교 컴퓨터과학과 학사과정
관심분야 : 보안, 블록체인

김 희 열 (Heeyoul Kim)

2000년 2월 : KAIST 컴퓨터과학과
2002년 3월 : KAIST 컴퓨터과학과(공학석사)
2007년 3월 : KAIST 컴퓨터과학과(공학박사)
2008년 : 삼성전자 수석엔지니어
2009년 3월 ~ 현재 : 경기대학교 컴퓨터공학부 부교수
관심분야 : 정보보호, 블록체인

김 남 기 (Namgi Kim)

1997년 2월 : 서강대학교 컴퓨터과학과
2000년 3월 : KAIST 전산학과(공학석사)
2005년 3월 : KAIST 전산학과(공학박사)
2007년 2월 : 삼성전자 통신연구소 책임연구원
2007년 3월 ~ 현재 : 경기대학교 컴퓨터공학부 교수
관심분야 : 통신시스템, 네트워크