암호화폐 무결성 거래를 위한 Whitelisting과 Hyperledger Fabric 재구성 기법

장수안[1], 이근호[2*]
[1]백석대학교 컴퓨터공학부 학생, [2]백석대학교 컴퓨터공학부 교수

A Scheme Reconfiguration of Whitelisting and Hyperledger Fabric for Cryptocurrency Integrity Transactions

Su-An Jang[1], Keun-Ho Lee[2*]
[1]Student, Division of Computer Engineering, Baek-seok University
[2]Professor, Division of Computer Engineering, Baek-seok University

요 약 암호화폐를 거래하기 위해서 거래자들은 개인의 암호화폐 지갑이 요구된다. 블록체인 기술을 활용한 암호화폐 그 자체는 우수한 보안성과 신뢰성을 보장받고 있어 블록체인 해킹 위협은 거의 불가능하지만, 거래자들이 거래를 위해 사용하는 거래소 환경에서 해킹 위협을 가장 많이 받고 있다. 거래 과정에서 블록체인을 통해 안전하게 거래가 이루어진다 해도 거래자의 지갑 정보 자체가 해킹되면 이와 같은 과정들에서 보안을 확보할 수 없다. 거래소 해킹은 주로 거래자의 지갑 정보를 탈취함으로써, 해커가 피해자의 지갑 자산에 접근이 가능해지므로 이루어진다. 본 논문에서는 이를 방지하고자 기존 Hyperledger Fabric 구조를 재구성하고, Whitelisting을 활용하여 거래 과정에서 거래자의 신원 무결성을 검증하는 시스템을 제안하고자 한다. 해당 과정을 거쳐 해커에 의한 암호화폐 자산 피해를 방지하고 인지할 수 있다는 장점이 있다. 또한, 기존 Hyperledger Fabric에서 피해자의 지갑 정보가 탈취되었을 경우 발생할 수 있는 거래 과정의 문제점을 지적하고 이를 보완하고자 한다.

주제어 : 하이퍼레저 페브릭, 화이트리스트, Chaincode, Orderer, Peer, 거래

Abstract To trade cryptocurrency, traders require a personal cryptocurrency wallet. Cryptocurrency itself using blockchain technology is guaranteed excellent security and reliability, so the threat of blockchain hacking is almost impossible, but the exchange environment used by traders for transactions is most subject to hacking threats. Even if transactions are made safely through blockchain during the transaction process, if the trader's wallet information itself is hacked, security cannot be secured in these processes. Exchange hacking is mainly done by stealing a trader's wallet information, giving the hacker access to the victim's wallet assets. In this paper, to prevent this, we would like to reconstruct the existing Hyperledger Fabric structure and propose a system that verifies the identity integrity of traders during the transaction process using whitelisting. The advantage is that through this process, damage to cryptocurrency assets caused by hackers can be prevented and recognized. In addition, we aim to point out and correct problems in the transaction process that may occur if the victim's wallet information is stolen from the existing Hyperledger Fabric.

Key Words : Hyperledger Fabric, Whitelist, Chaincode, Orderer, Peer, Transaction

*교신저자 : 이근호(leekeunho1004@gmail.com)
접수일 2023년 12월 27일 수정일 2024년 01월 25일 심사완료일 2024년 01월 28일

1. 서론

암호화폐를 거래하기 위한 거래소 플랫폼에 저장된 거래자의 지갑 주소에 대한 정보 데이터베이스가 해커에 의해 유출이 일어나면, 해커는 피해자의 지갑에 접근할 수 있고, 여기서 피해자의 자산이 유출될 수 있다.

이 문제점을 해결하기 위해, Hyperledger Fabric 구조를 재구성하여, 거래 과정에서 거래자의 신원 무결성을 검증하여 거래에 참여한 거래자가 지갑 주인임을 증명한다. 거래가 진행되기 전에, 거래자가 지갑 주소를 생성할 때 사용한 이메일을 통한 2차 인증을 진행하여 거래의 무결성을 입증한다. 이 과정에서 이메일 Whitelisting을 활용한다. 지갑 주인의 이메일은 재구성된 Hyperledger Fabric 네트워크에 존재하는 Private 블록체인의 Whitelist DB에 보관하여 인증된 이메일 이외에는 거부하고, 2차 인증은 Private 블록체인에 접근 가능한 허가된 관리자인 Orderer를 통해서만 인증 가능한 구조를 제안한다.

Hyperledger Fabric을 사용하는 이유는 다음과 같다. 먼저, Fabric 내부에서 채널을 사용하여 거래를 진행하므로, 블록체인의 네트워크 구조의 분할이 가능하다.

또한, State 데이터베이스라는 데이터 저장소에 거래 실행 직후 결과 상태를 저장한다. 이를 통해 모든 블록체인을 확인할 필요 없이 특정 시점의 상태를 확인할 수 있도록 한다.

기존 Hyperledger Fabric에서, 피어에 사용자가 접근하기 위해 MSP(Membership Service Provider)를 통한 CA 인증 기관을 거쳐 접근할 수 있다. 하지만, 지갑 주인의 개인키가 탈취되어 공격자가 접근이 가능한 경우, 지갑 주인의 자산을 옮기기 위해 Peer에 접근할 수 있다.

따라서, Hyperledger Fabric에서 거래자들 Orderer와 통신하여, 실제 거래를 진행하는 거래자가 자신의 지갑 주인임을 증명하는 2차 인증 과정을 추가하여 거래 과정의 무결성과 신뢰성을 보장한다.

Orderer는 Hyperledger Fabric 구조에 존재하는 Private 블록체인 내부에, 거래자들이 지갑 주소를 생성할 때 사용한 이메일을 저장한 데이터베이스를 위치하여, 여기서 2차 인증을 진행하도록 한다. 만약, 지갑 주인의 개인키가 탈취되어 공격자가 거래를 진행하더라도, Private 블록체인 내부의 저장된 이메일로부터 2차 인증이 통과되지 않는다면 거래가 무효가 된다. 여기서 이메일 Whitelisting을 통해 데이터베이스에 등록된 이메일이 아닌 다른 이메일은 차단하여 2차 인증의 신뢰성을 보장한다.

이에 따라 본 논문에서는 암호화폐 지갑 주인의 개인키가 탈취당하여 거래가 진행될 때, Hyperledger Fabric 구조를 재구성하고 이메일 Whitelisting을 적용하여, 암호화폐 거래 과정에서 무결성과 신뢰성을 보장할 수 있는 방식을 제안하고자 한다.

2. 관련연구

2.1 Hyperledger Fabric

Hyperledger Fabric은 허가형 Private 블록체인의 형태를 가진다. 누구나 자유롭게 참여 가능한 Public 블록체인 환경과 달리, 인증 관리 구조에 의해 허가된 신뢰있는 사용자만이 Hyperledger Fabric 블록체인 네트워크에 참여할 수 있다.

Hyperledger Fabric에서는 모든 노드가 동일한 ledger 정보를 공유하여 활용하고, 비즈니스 취지에 맞게 사용하고자 하는 노드 간에 별도의 ledger를 생성하는 것이 가능하다[1-3].

2.2 Chaincode

Chaincode는 분산원장에 데이터를 기록하거나 읽기 위해서 사용하고, Peer 내에 존재하는 State 데이터베이스를 조회할 수 있다. 주로 Smart Contract를 위해 전용 Container에서 실행된다. 여러 개의 Chaincode를 만들 수 있으며, 하나의 Chaincode에서 다른 Chaincode를 호출할 수 있다.

Hyperledger Fabric에서 기본적으로 제공되고, 시스템 레벨에서 수행되는 Chaincode를 System Chaincode로 분류하며, 5가지의 Chaincode 종류가 존재하여 운영된다[4-6].

2.3 Peer

Peer는 원장과 Chaincode를 관리하는 역할을 하는 노드로, Hyperledger Fabric 네트워크에서 트랜잭션이 원장에 반영되는 과정에서 필요한 노드이다.

Peer는 기본적으로 Docker 컨테이너로 구성되어 있어, 네트워크 기동 시 각 노드들의 Docker 이미지를 통해 Docker 컨테이너를 실행하도록 한다.

Peer의 원장과 Chaincode는 기본적으로 Peer의 Docker 컨테이너 안에 위치하므로, Peer를 통해서만 분

산원장과 Chaincode에 접근할 수 있다.

필요에 따라 Peer는 복수의 분산원장과 Chaincode를 가질 수 있는 특징이 존재한다[7,8].

2.4 Orderer

기존 Orderer는 총 세 단계로 구분되어 진행된다.

DApp에서 트랜잭션 보증을 담당하는 Endorsing Peer에게 트랜잭션을 제출하는 것부터 해당 트랜잭션이 가리키는 Chaincode가 실행되는 것까지 1단계 과정으로 수행된다.

이후, 제출된 트랜잭션은 Orderer에 의해 수집되고, 이를 순서대로 정렬하여 최신 블록을 생성하는 과정을 블록 패키징이라 부르며 2단계 과정에 해당한다.

마지막 3단계로, Orderer는 생성한 최신 블록을 각 조직의 Peer에게 전달하여 관리하고, 최신 블록을 전달받은 Peer에 해당 블록이 올바르게 생성됐는지 검증하는 과정을 이행한다[9-11].

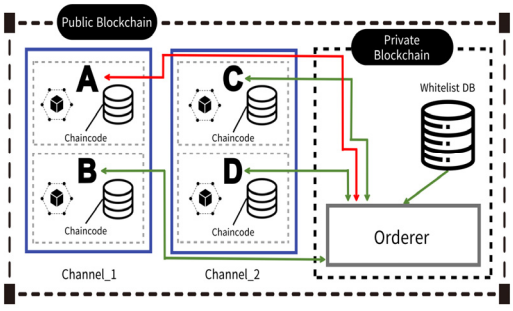
2.5 Whitelist

보안에서 Whitelist란, 모든 기본 정책이 차단된 상황에서 예외적으로 접근이 허락된 대상을 지정하는 방식 또는 여기에 할당된 대상들을 말한다,

이러한 맥락에서, Whitelisting의 일반적인 의미는 특정 IP 주소가 어떤 사이트에 접근하는 과정에서 사이트의 보안 프로세스에 의해 차단되지 않도록 하거나, 특정 수신자의 이메일이 자동으로 스팸 처리되지 않게 하도록 수동 절차를 거치는 것을 의미한다[12,13].

3. 본론

3.1 Hyperledger Fabric 재구성 구조



[Fig. 1] Hyperledger Fabric Reconfiguration Structure

본 논문에서는 기존 Hyperledger Fabric의 구조를 재구성하고, Whitelisting을 적용하여 거래 과정에서 거래자의 신원 무결성을 검증하고자 한다. 먼저 Hyperledger Fabric은 허가형 Private 블록체인 구조로, 누구나 자유롭게 참여가 가능한 기존의 Public 블록체인과 달리 Hyperledger Fabric에서는 인증 관리 시스템에 의해 허가된 사용자만이 블록체인 네트워크에 참여할 수 있다. 이를 통해, Fabric 네트워크에 참여한 노드들은 이미 신뢰를 가진 노드로 판단하여 구성된다.

먼저, 위의 [Fig. 1]에서 거래자 A, B가 거래를 하기 위해 Fabric 네트워크에 참여한 상태이다. 거래자 A, B는 기존 Hyperledger Fabric에서 사용되는 CA 인증을 거쳐 접근한다. 각각의 거래는 일대일 구조로, 각각의 거래자들의 Peer가 생성되고, 거래자들의 Peer가 모여 하나의 Channel을 구성한다. Peer 내부에는 해당 거래자들의 이전 거래 내용과 정보를 포함하는 데이터베이스인 State 데이터베이스가 존재한다. 또한, 이 State 데이터베이스를 조회하여 거래자의 비인가 행동과 이전 행적을 조회할 수 있는 Chaincode가 포함되어 있다.

거래자 A, B가 거래를 진행하려면 재구성된 Hyperledger Fabric 구조에 존재하는 Orderer와 Whitelist DB를 통해 거래자의 신원 무결성을 검증하는 과정을 거쳐야 한다. 여기서, CA 인증을 받은 거래자들이 참여하는 허가된 Public 블록체인 내부에 조직에서 인가된 사용자만이 접근할 수 있는 Private 블록체인 네트워크가 존재한다.

이 Private 블록체인에 Orderer와 Whitelist DB가 존재한다. 거래자 A, B가 거래를 요청하면, Orderer는 각 거래자의 State 데이터베이스를 확인하여 이전 거래 정보와 비인가 행동이 존재하는지 확인한다. Orderer는 Private 블록체인 내부에 존재하는 Whitelist DB에 접근할 수 있는 유일한 사용자로, 이 Whitelist DB에는 거래자의 지갑 주소 정보와 지갑을 생성할 시 인증에 사용한 이메일 정보를 포함하고 있다.

Orderer는 거래자 A, B의 지갑 주소 정보와 이메일 정보를 확인하고, 이를 2차 인증에 활용하여 현재 거래에 참여한 거래자 A, B가 정말 본인이 직접 거래에 참여하는지 확인한다.

3.2 CA 인증 문제

기존 Hyperledger Fabric 구조에서 거래자들은 Peer에 접근하기 전에 CA 인증을 통과하여 접근한다. 하지만, 해커에 의해 지갑 주인의 정보가 유출되면, 지갑의 개인 키와 인증서들이 유출되고 Fabric 네트워크에

참여 과정에서 거래자 신원의 무결성을 확보할 수 없다. 그 결과 해커는 CA 인증을 통과하여 지갑 주인의 자산을 탈취하기 위한 거래가 진행될 수 있다는 문제점이 존재한다.

이를 방지하기 위해, 재구성된 Hyperledger Fabric에는 내부에 조직의 인가된 사용자만 접근 가능한 Private 블록체인 네트워크를 조성하고, Whitelist DB를 통해 거래자의 신원 무결성을 검증한다[14,15].

3.3 Whitelist DB

재구성된 Hyperledger Fabric에는 거래자의 신원 무결성 검증을 위해 Whitelist DB를 구성한다. 이 Whitelist DB의 역할은 각 Peer에 입장한 거래자들의 지갑 생성 시 인증에 사용한 이메일 정보 저장을 진행한다.

거래자의 지갑 생성 시 인증에 사용한 이메일을 저장하여 거래의 허가를 위해 Orderer로부터 2차 인증을 통과하는데, 이때 활용하는 지갑 생성 시 인증에 사용한 이메일로부터 인증을 진행하여 현재 거래에 참여하고 있는 거래자가 지갑의 주인인지 확인한다. Whitelist DB에 포함되지 않은 이외의 이메일은 모두 배제되며, 이는 인증 우회를 방지하기 위해 Whitelisting을 진행한다.

2차 인증을 통과하지 못한다면, 현재 거래에 참여한 거래자는 지갑의 주인이 아닌 제3자가 관여하고 있음을 확인할 수 있다. 또한, 양측 거래자들이 2차 인증을 통과하지 못할 경우, 그 즉시 거래는 진행되지 않고 무효가 된다.

4. 재구성된 Hyperledger Fabric에서 거래 과정

재구성된 Hyperledger Fabric에서 거래자들의 거래 과정은 [Fig.2]와 같다.

Step 1. 거래를 원하는 거래자 A, B가 재구성된 Hyperledger Fabric에 CA 인증을 거쳐 참여한다.

Step 2. 입장한 각각의 거래자들의 이전 거래 내용과 정보들을 가진 State 데이터베이스와, 이를 조회할 수 있는 Chaincode 가 존재하는 Peer에 입장한다.

Step 3. 거래는 일대일로 이루어지므로, 거래자 A, B의 Peer가 하나의 Channel로 묶여 거래를 준비한다.

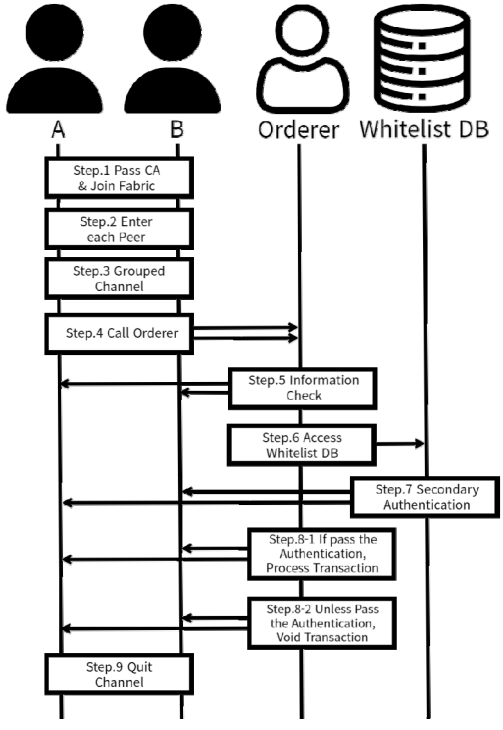
Step 4. 거래의 진행을 위해 재구성된 Hyperledger Fabric 내부의 Private 블록체인에 접근 가능한 관리자인 Orderer를 호출하여 거래를 진행한다.

Step 5. Orderer는 거래자 A, B의 정보를 거래자들의 Peer에 존재하는 Chaincode를 활용하여 State 데이터베이스 정보를 검사한다.

Step 6. 거래자의 정보를 확인한 Orderer는 재구성된 Hyperledger Fabric 내부의 Private 블록체인에서 Whitelist DB에 접근한다.

Step 7. 거래자 A, B에 대한 2차 인증을 진행하기 위해 Whitelist DB에 저장된 A, B에 대한 지갑 생성 시 활용한 인증 이메일을 통해 2차 인증을 이행한다.

Step 8-1. 거래자들이 2차 인증을 통과할 시, 거래자의 신원 무결성 검증이 보장됐으므로, Orderer는 거래자 A, B에 대한 거래를 진행한다.



[Fig. 2] Transaction Process in Hyperledger Fabric Reconfiguration Structure

Step 8-2. 거래자 중 2차 인증을 통과하지 못한 거래자가 존재할 시, 거래자의 신원 무결성 검증이 보장되지 않으므로, Orderer는 거래자 A, B에 대한 거래를 중지하고 거래를 무효로 한다.

Step 9. 거래가 종료된 후, 각각의 거래자들의 Peer에 존재하는 State 데이터베이스에 진행된 거래에 대한 정보들이 저장되고, 거래자들은 거래가 진행된 Channel에서 벗어난다.

위와 같은 아홉 단계를 통해 순차적인 거래가 진행되며, Step 8-1과 8-2에서 Whitelist 인증이 허가된 경우와 그렇지 아니한 경우의 구별된 진행을 통해 거래의 허가와 무효를 결정한다. 이를 통해 암호화폐 거래자에 대한 무결성과 신뢰성을 보장할 수 있다.

5. 결론

본 논문에서는 기존 Hyperledger Fabric 구조를 재구성하고, Whitelisting을 적용하여 암호화폐 무결성 거래 시스템을 제안하였다. 본 논문에서 제안된 시스템을 적용할 경우 발생하는 기대효과는 다음과 같다.

암호화폐 거래소에서 거래자의 지갑 정보들이 해커에 의해 유출되었다고 가정했을 때, 해커가 피해자들의 지갑 자산을 탈취하는 과정에서 본 논문에서 제시한 재구성된 Hyperledger Fabric 구조가 이를 방지할 수 있다.

기존 Hyperledger Fabric 구조에서 해커는, 피해자의 지갑 정보를 활용하여 CA 인증을 통과하고 피해자의 거래 이력이 존재하는 Peer에 손쉽게 접근하여 거래를 이행할 수 있다.

하지만, 재구성된 Hyperledger Fabric 구조에서는 거래가 이행되기 전, 조직에서 인가된 사용자이자, Hyperledger Fabric 네트워크의 중앙관리자인 Orderer에 의해 2차 인증이 통과해야 거래가 허가된다. 여기서 재구성된 Hyperledger Fabric 구조에 존재하는 내부 Private 블록체인에 Whitelist DB가 이를 검증한다.

중앙관리자인 Orderer만이 접근할 수 있는 내부 Private 블록체인에 존재하는 Whitelist DB는, 거래자의 지갑을 생성할 시 활용한 인증 이메일 정보들이 저장되어 있다. 이는 거래자가 Orderer로부터 2차 인증을 이행하기 위한 이메일 정보이며, Whitelist DB에 포함되지 않는 이메일들은 모두 배제하여 인증 우회를 방지하기 위한 목적이다.

해당 인증을 통과하지 못하면 즉시 거래는 중지되고 무효화 된다. 이를 통해, 지갑 정보를 유출 당한 피해자의 자산을 보호하고, 해커의 악의적인 행동을 저해할 수 있다고 판단한다.

또한, Hyperledger Fabric 구조의 특징인 비즈니스 목적에 부합하는 노드간의 별도의 원장을 생성하는 점을 특화하여 향후 비즈니스 거래에서 Hyperledger Fabric 재구성 구조를 연구할 수 있다고 판단한다.

REFERENCES

[1] B. Hofmann, P. Kasinathan and M. Wimmer, "Towards achieving confidentiality in Hyperledger Fabric," in 2022 IEEE International Conference on Blockchain (Blockchain), pp.384-391, 2022.

[2] M. Graf, R. Küsters and D. Rausch, "Accountability in a Permissioned Blockchain: Formal Analysis of Hyperledger Fabric," 2020 IEEE European Symposium on Security and Privacy (EuroS&P), pp.236-255. 2020.

[3] M. Kwon and H. Yu, "Performance Improvement of Ordering and Endorsement Phase in Hyperledger Fabric," 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), pp.428-432, 2019.

[4] L. Foschini, A. Gavagna, G. Martuscelli and R. Montanari, "Hyperledger Fabric Blockchain: Chaincode Performance Analysis," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), pp.1-6, 2020.

[5] Mohan M, Smitha and L. Sujihelen. “AN EFFICIENT CHAIN CODE FOR ACCESS CONTROL IN HYPER LEDGER FABRIC HEALTHCARE SYSTEM.” e-Prime - Advances in Electrical Engineering, Electronics and Energy (2023).

[6] D.J.Park, H.A.Song, H.S.Eom, S.M.Jeong, J.S.Park, and K.H.Yeom, "A Smart Contract Management System to Optimize Transactions in a Permissioned Blockchain," KIISE Transactions on Computing Practices, Vol.28, No.6, pp.360-365, 2022.

[7] Ning Lu, Yongxin Zhang, Wenbo Shi, Saru Kumari, Kim-Kwang Raymond Choo, A secure and scalable data integrity auditing scheme based on hyperledger fabric, Computers & Security, Vol.92, 2020.

[8] H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi and A. Rindos, "Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network (Hyperledger Fabric)," 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), pp.253-255, 2017.

[9] Xiaojie Zhao, Shangping Wang, Yaling Zhang, Yu Wang, Attribute-based access control scheme for data

sharing on hyperledger fabric, Journal of Information Security and Applications, Vol.67, 2022.

[10] L. Alashaikh, "Blockchain-Based Software Systems: Taxonomy Development," 2021 IEEE International Conference on Blockchain (Blockchain), pp.491-498. 2021.

[11] U. Goel, DR. Sonanis, I. Rastogi, S. Lal and A. De, "Criticality Aware Orderer for Heterogeneous Transactions in Blockchain," 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp.1-4. 2020.

[12] Vesely, A., "DNS Whitelist (DNSWL) Email Authentication Method Extension", RFC 8904, 2020.

[13] Nureni Ayofe Azeez, Sanjay Misra, Ihotu Agbo Margaret, Luis Fernandez-Sanz, Shafi'i Muhammad Abdulhamid, Adopting automated whitelist approach for detecting phishing attacks, Computers & Security, Vol.108, 2021.

[14] Yue Li, Mingcheng Xu, and Gaojian Xu. 2022. Blockchain-based mutual authentication protocol without CA. J. Supercomput. 78, 15, pp.17261–17283. 2022.

[15] Sinha, A. and Sadhya, D. Decentralized Public Key Infrastructure with Identity Management using Hyperledger Fabric. In Proceedings of the 19th International Conference on Security and Cryptography-SECRYPT; SciTePress, pp.554-559, 2022.

장 수 안(Su-An Jang) [준회원]

■ 2023년 3월 ~ 현재 : 백석대학교 컴퓨터공학부

〈관심분야〉
취약점 분석, 디지털 포렌식, 융합보안, 블록체인

이 근 호(Keun-Ho Lee) [종신회원]

■ 2006년 8월 : 고려대학교 컴퓨터학과(이학박사)
■ 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 기술전략팀 과장
■ 2010년 3월 ~ 현재 : 백석대학교 컴퓨터공학부 교수

〈관심분야〉
융합보안, 블록체인, 개인정보보호, 이동통신 보안