Hyperledger Indy 기반의 DID와 EMR 통합 시스템 기법

양지용[1], 엄효상[1], 이근호[2*]
[1]백석대학교 컴퓨터공학부 학생, [2]백석대학교 컴퓨터공학부 교수

A Scheme for DID and EMR Integrated System based on Hyperledger Indy

Jiyong Yang[1], Hyosang Eom[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 의료 서비스의 효율성과 질은 개인의 의료 정보의 안전한 보호와 투명한 관리에 크게 의존하며, 이는 디지털 시대에 더욱 중요해지고 있다. 현재의 EMR 시스템은 중앙 집중식으로 운영되어 개인의 의료 정보에 대한 소유권 및 투명성 부족으로 인해 문제가 발생하고 있으며 데이터 공유 및 업데이트 과정에서 지연과 오류가 발생할 수 있다. 이러한 문제를 해결하기 위해, Hyperledger Indy 기반의 분산 신원 관리(DID)와 전자 의료 기록(EMR) 통합 시스템을 제안한다. 이 시스템은 의료 정보의 소유권을 개인에게 확실히 보장하고, 의료 정보의 접근성과 활용도를 높이는 데 목표를 두고있다. 개인은 이 시스템을 통해 자신의 의료 정보를 직접 관리하고, 필요한 경우 해당 정보를 투명하게 공유할 수 있게 되어, 의료 서비스의 효율성을 높일 수 있다. 또한, 이 시스템은 의료 정보를 안전하게 보호하고, 투명하게 관리하여, 의료 서비스의 투명성을 높이고, 개인의 의료 정보에 대한 통제력을 강화한다. 따라서, 이 시스템은 의료 서비스의 질 향상, 개인의 의료 정보 보호, 그리고 의료 서비스의 효율성 향상에 크게 기여할 것이다.

주제어 : Hyperledger Indy, DID, EMR, Indy Plenum, Ledger

Abstract The efficiency and quality of healthcare services rely heavily on the secure protection and transparent management of individuals' medical information, which is becoming increasingly important in the digital age. To address this issue, we propose a distributed identity management (DID) and electronic medical record (EMR) integration system based on Hyperledger Indy, which aims to ensure the ownership of medical information to individuals and increase the accessibility and utilization of medical information. The system will allow individuals to manage their own medical information and share it transparently when necessary, which will improve the efficiency of healthcare services. In addition, the system will securely protect and transparently manage medical information, increasing the transparency of medical services and strengthening individuals' control over their medical information. Thus, the system will contribute significantly to improving the quality of medical services, protecting individuals' medical information, and improving the efficiency of medical services.

Key Words : Hyperledger Indy, DID, EMR, Indy Plenum, Ledger

*교신저자 : 이근호(leekeunho1004@gmail.com)
접수일 2024년 01월 17일 수정일 2024년 02월 10일 심사완료일 2024년 02월 13일

1. 서론

현대 사회에서 의료 서비스는 개인의 건강을 유지하고, 질병을 예방하며, 치료하는 데 있어 핵심적인 역할을 수행하고 있다. 그러나 의료 서비스의 질과 효율성은 개인의 의료 정보를 얼마나 잘 관리하고 활용하는지에 크게 좌우된다. 이런 맥락에서, 의료 정보의 안전한 보호와 투명한 관리는 절대적인 중요성을 띠고 있다. 더욱이, 디지털 시대에 접어들며 이들 의료 정보는 전자화되어 다양한 형태로 활용되고 있어, 그 중요성은 더욱 강조되고 있다.

이러한 문제 해결을 위해 Hyperledger Indy 기반의 분산 신원 관리(DID)와 전자 의료 기록(EMR) 통합 시스템을 구성하고자 한다. 이 시스템은 의료 서비스의 투명성과 안전성을 극대화하며, 의료 정보의 소유권을 개인에게 확실히 보장하는 동시에 개인의 의료 정보에 대한 접근성과 활용도를 높이는 데 목표를 두고 있다.

Hyperledger Indy는 분산 레지스트리를 통해 각 개인의 식별 정보를 보호하며, 개인이 직접 자신의 정보를 관리하고 공유하는 것을 가능하게 하는 도구이다. 이를 의료 서비스에 접목시키면, 개인은 자신의 의료 정보를 직접 관리하고, 필요한 경우 해당 정보를 투명하게 공유할 수 있게 된다. 이는 개인의 의료 정보에 대한 소유권과 통제력을 강화하며, 의료 서비스의 효율성을 높일 수 있다.

한편, 전자 의료 기록(EMR)은 개인의 의료 정보를 디지털화하여 저장, 관리, 분석하는 시스템으로, 의료 서비스의 질을 높이고, 의료 비용을 줄이는 데 기여하고 있다. 이 시스템과 DID를 통합하면, 개인의 의료 정보를 더욱 안전하게 보호하고, 투명하게 관리할 수 있게 된다.

이러한 통합 시스템은 개인의 의료 정보를 보호하고, 의료 기관과 개인간의 정보 공유를 원활하게 하여, 의료 서비스의 효율성을 높이는 데 기여할 것이라고 생각한다. 또한, 이 시스템은 의료 정보를 개인이 직접 관리하고, 필요에 따라 선택적으로 공유할 수 있도록 하여, 의료 서비스의 투명성을 높이고, 개인의 의료 정보에 대한 통제력을 강화할 것이라고 예상한다.

따라서, Hyperledger Indy 기반의 DID와 EMR 통합 시스템 기법을 통하여 의료 서비스의 질을 향상시키고, 개인의 의료 정보를 보호하며, 의료 서비스의 효율성을 높이고자 새로운 방식의 시스템 기법을 구성하고자 한다.

2. 관련연구

2.1 Hyperledger Indy

Hyperledger Indy는 신원 관리 분야에서 사용되는 오픈 소스 블록체인 프로젝트로 분산된 신원 관리 시스템을 구현하기 위한 플랫폼으로 개발되었다.

주로 디지털 신원 및 신원 관리에 중점을 둔 Hyperledger Indy는 분산 원장 기술을 기반으로 하여 보안성과 탈중앙화를 강조하고 있다[1].

또한 Hyperledger Indy는 금융 서비스와 같은 신원에 있어 중요한 서비스들에 대하여 지속적으로 연구하여 사용하고 있다.

Hyperledger Indy는 Verifiable Credentials와 Zero-Knowledge Proofs와 같은 암호학적 기술을 사용하여 사용자가 필요한 만큼의 정보를 공유하면서도 개인 정보를 최대한 보호할 수 있는 환경을 제공한다[2].

이를 통하여 사용자는 필요한 신원 정보를 제공하고 인증할 수 있으며, 민감한 개인 정보는 블록체인에서 안전하게 보호된다. Hyperledger Indy의 합의 알고리즘으로는 Indy Plenum이 사용되며, Indy Plenum은 높은 신뢰성과 내결함성을 제공하는 분산 컨센서스 알고리즘이다. 이러한 기술적 특성은 분산 환경에서 안전하게 운영되고 무결성을 유지할 수 있는 기반을 제공한다[3, 4].

2.2 Indy Plenum 합의 알고리즘

Indy Plenum은 분산된 시스템에서 합의를 도출하기 위한 알고리즘이다. 해당 알고리즘은 오픈 소스인 Hyperledger Indy에서 사용되며, 퍼블릭 블록체인 네트워크를 구축하는 데 사용된다[5].

Indy Plenum은 비잔틴 장애 허용(BFT) 합의 알고리즘으로 알려져 있으며 이는 분산된 시스템에서 장애가 발생할 수 있는 환경에서도 합의를 도출할 수 있는 알고리즘이다[6].

Indy Plenum은 3가지의 주요한 개념을 기반으로 작동한다.

첫째, 합의를 도출하기 위하여 노드들은 통신을 통하여 정보를 교환한다. 이때, 노드들은 메시지를 서명하여 신원을 검증하며, 메시지의 순서를 지정하기 위해 합의된 규칙을 따른다.

둘째, Indy Plenum은 투명성을 보장하기 위해 블록체인을 사용한다. 이 블록체인은 모든 참여자들에게 공유되며, 이를 통하여 노드들은 합의된 트랜잭션의 유효성을 확인하고, 변조를 감지할 수 있다.

셋째, Indy Plenum은 비잔틴 장애를 허용하는 알고리즘으로 설계되었다. 비잔틴 장애란 시스템에 장애를 일으키려는 악의적인 노드의 존재를 의미하여 Indy Plenum은 이러한 악의적인 노드들에 대해서도 합의를 도출할 수 있도록 설계되었다.

즉 Indy Plenum은 분산된 시스템에서 합의를 도출하기 위한 알고리즘으로, 정보 교환, 투명성, 비잔틴 장애 허용을 기반으로 작동하여 이를 통하여 안정성과 신뢰성이 요구되는 네트워크에서 합의를 도출할 수 있다.

2.3 DID

DID(Distributed Identifier)은 분산 식별자로, 개인의 신원을 고유하게 식별하기 위한 기술이다. DID는 중앙 집중식 신원 인증 방식이 아닌 분산형으로 운영되며 개인의 신원 정보를 안전하게 관리하고 공유할 수 있고, 자신의 DID를 생성하고 소유하여 필요한 신원 정보를 안전하게 보관할 수 있다.

[Fig. 1] DID Schema

DID의 주요 특징 중 하나는 분산형 관리다. 일반적으로 신원을 검증하기 위해서는 중앙화된 기관의 확인이나 검증이 필요하지만 DID는 중앙화된 기관이나 중개자 없이 개인이 직접 DID를 생성하고 소유할 수 있다. 이는 개인 신원 정보의 주권과 자기결정권을 부여하며, 개인의 신원 정보가 중앙 집중식 시스템에 의존하지 않고 안전하게 관리될 수 있도록 한다.

또한, DID는 개인정보 보호에 큰 역할을 한다. 개인의 신원 정보는 블록체인과 같은 분산형 장부에 저장되거나 암호화되어 보호되며, 개인정보 유출의 위험을 최소화하고 개인의 데이터 소유권을 강화할 수 있다.

또한, 필요한 경우에만 개인의 신원 정보를 제공하고 검증할 수 있으므로 개인은 불필요한 개인정보 제공을 피할 수 있다 [7]. DID는 표준화된 형식으로 정의되어 있어 다른 시스템과 연계하여 신원 정보를 안전하게 교환할 수 있다. 이는 다양한 플랫폼과 서비스 간에 신원 인증을 원활하게 수행할 수 있도록 도와준다 [8].

개인은 자신의 DID를 사용하여 다양한 온라인 서비스에서 신뢰성 있는 신원 인증을 받을 수 있다.

DID 신원 인증 기술은 개인의 신원 정보를 안전하게 관리하고 상호 운용성을 제공하는 혁신적인 기술이다. 이를 통해 개인은 자신의 신원을 소유하고 통제할 수 있으며, 안전하고 신뢰성 있는 거래를 실현할 수 있다.

또한 데이터 활용과 중요성이 점차 커져가는 현대에서 데이터를 이용해 악용하는 사례들이 늘고있어 개인정보를 관리하며 대규모 개인정보 유출 위험과 개인정보를 악용한 범죄를 막기 위해 최근 DID 기술의 대부분은 의료기록 관리, 신원인증, 금융거래 등과 같은 서비스에서 활용되고 있다.

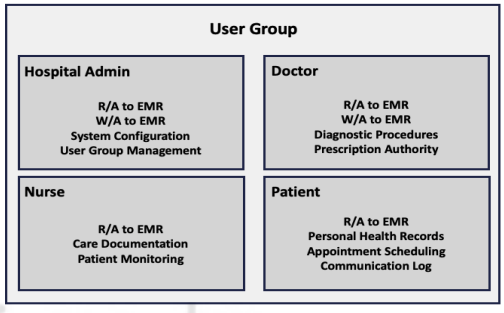
2.4 EMR

EMR 데이터는 의료기록을 전자 문서 형태로 기록 및 보존하는 것을 의미한다. 과거에는 다양한 의료기관에서 환자의 인적 사항, 병력, 환자의 진료 기록, 처방, 이미지 차트 등 환자의 모든 정보를 종이 문서 형태로 보관했다. 하지만 관리자의 부주의로 인해 유실이 발생하거나 종이 문서의 특성상 시간이 지남에 따라 관리가 어려워졌다. EMR 데이터에는 환자의 진료 기록, 처방, 이미지 차트 등 매우 중요한 내용이 저장되어 있어 의료기관이나 의료 전문가들이 필요할 때 쉽게 접근할 수 있으며 아래 사진과 같이 중앙 집중형 방식으로 데이터를 저장하고 있다[9].

이러한 저장 방식은 모든 데이터가 서버 중앙에 저장되기 때문에 악의적인 사용자로부터 보안 위협이 발생할 수 있다. 또한, EMR 시스템은 환자의 개인 정보와 밀접하게 연관되어 있기 때문에 권한을 가진 사람만 접근할 수 있도록 보안에 대한 필요성이 매우 중요하다.

3. 본론

3.1 Hyperledger Indy 사용자 그룹 별 권한



[Fig. 2] Permissions by user group

제안하고자 하는 시스템에서는 [Fig 2]와 같이 사용자 그룹 별 권한을 두어 사용자에 따라 EMR 데이터에 접근할 수 있는 데이터를 나눈다.

[Fig. 2]에서 볼 수 있듯이 R/A to EMR(Read Access to EMR)과 W/A to EMR(Write Access to EMR) 등과 같이 각 그룹 별 EMR 데이터에 접근할 수 있는 권한에 제한이 있다.

3.1.1 병원장

병원장은 전체 병원 시스템에서 가장 높은 권한을 보유한 주체로, [Fig 2]에서 확인할 수 있는 대로 EMR 데이터에 대한 전체적인 통제 권한을 갖는다.

이는 병원 전반의 데이터 접근 및 조작 권한을 포함하며, 신뢰성과 보안성을 유지하면서 전반적인 시스템 관리에 참여한다.

3.1.2 의사

의사는 EMR 데이터에 대한 접근 권한이 있으며, 이는 병원장보다는 한 단계 낮은 권한 수준을 의미한다. 의사는 자신의 환자 데이터에 대한 접근 및 수정이 가능하며, 치료 및 진단을 위한 필요한 정보를 확인할 수 있다. 이를 통해 의료 서비스의 빠른 의사 결정 및 효과적인 치료가 가능하다.

3.1.3 간호사

간호사는 EMR 데이터에 대한 한정적인 권한을 가진다. 주로 환자의 일상적인 관리와 간호 활동에 필요한 정보를 열람하고 기록하는 역할을 수행하며 간호사의 권한은 의사보다는 낮지만, 환자의 건강 상태에 대한 중요한 정보를 공유하며 환자 전반의 케어를 지원한다.

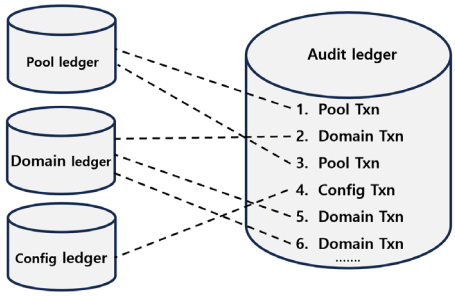
3.1.4 환자

환자는 자신의 EMR 데이터에 대한 일부 권한을 가지며, 주로 자신의 건강 정보를 확인하고 관리하는 데 사용한다. Hyperledger Indy의 DID를 기반으로 한 신원 관리 시스템을 통해 개인이 자신의 데이터에 대하여 투명하고 안전한 접근을 유지할 수 있다.

3.2 원장 별 데이터 처리 과정

원장 별 데이터 처리는 Hyperledger Indy 기반의 DID와 EMR 통합 시스템에서 핵심적인 부분으로, Pool Ledger, Domain Ledger, Config Ledger의 각각의 특성을 고려하여 구성되어야 한다. 이러한 Pool Ledger, Domain Ledger, Config Ledger에서 발생한 트랜잭션은 서로에게 의존성이 있기 때문에 Audit Ledger에서 순서대로 취합하여 저장한다.

아래는 원장 별 데이터 처리 과정에 대한 세부 내용이다[10].



[Fig. 3] Audit Ledger 트랜잭션

3.2.1 Pool Ledger 데이터 처리 과정

Pool Ledger에는 네트워크에 참여하는 노드들의 등록 정보가 저장된다.

새로운 참여자가 네트워크에 가입하면, 이 정보는 Pool Ledger에 기록되어 전체 네트워크에 공유된다.

분산된 노드 간 동기화가 이루어지는 Pool Ledger는 분산 원장으로서, 노드들 간 일관성을 유지하고 데이터의 동기화를 보장하며 새로운 블록이 추가되거나 변경사항이 있을 때, 이를 모든 노드에 동시에 전파하여 불변성과 일관성을 유지한다[11].

3.2.2 Domain Ledger 데이터 처리 과정

DID 관리 및 신원 정보 기록은 Domain Ledger에서 신원 정보와 DID에 관련된 데이터가 저장된다. DID의 생성, 업데이트, 연결 등의 작업은 Domain Ledger에 기록되어 안전한 신원 관리를 제공한다.

또한 연결된 참여자 간 권한 관리는 참여자 간의 관계 및 권한은 Domain Ledger에서 관리되며 DID를 기반으로 한 권한 부여가 이루어져, EMR에 접근하고 데이터를 공유하는 권한이 부여된다.

3.2.3 Config Ledger 데이터 처리 과정

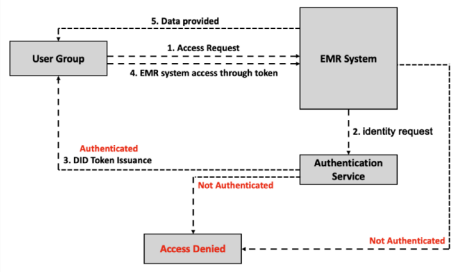
Config Ledger는 시스템의 설정 정보를 관리하며, 시스템 동작에 영향을 미치는 설정 사항이 기록된다.업데이트나 변경 사항은 Config Ledger에 기록되어 전체 네트워크에 투명하게 공유된다.

3.2.4 Audit Ledger

원장별 데이터 처리 과정에서는 Pool Ledger, Domain Ledger, Config Ledger에서 발생한 트랜잭션중 일부는 [Fig 3]과 같이 일부는 시퀀스 번호와 연결된 블록으로 간주될 수 있으며 Merkle Tree에 대한 참조도 있으므로 모든 트랜잭션의 실제 순서와 트랜잭션이 속한 원장을 복원할 수 있다. 이로써 안전하고 효율적인 DID 및 EMR 관리 시스템을 구축한다[12,13].

3.3 사용자 그룹 별 EMR 데이터 접근 과정

사용자 그룹은 EMR 시스템에 접근하여 데이터를 받기 위해 아래와 같은 접근 과정을 거치게 된다.



[Fig. 4] Permissions by user group

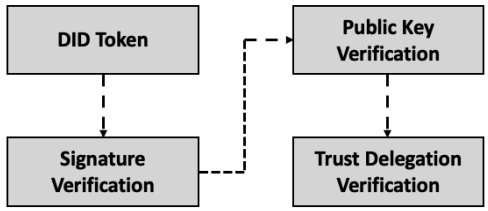
먼저 [Fig 4] 1번 Access Request와 같이 User Group에 포함된 사용자는 본인 또는 환자에 대한 EMR 데이터를 받기 위해 EMR 시스템에 접근 요청을 보내게 된다.

EMR 시스템은 접근 요청을 받으면 [Fig 4] 2번 Identity Request와 같이 인증 서비스에 사용자 그룹에 대한 신원을 요청한다.

다음으로는 만약 신원이 맞다면 DID 토큰을 User Group에 속한 User에게 전달을 해준다. 만약 신원이 맞지 않다면 인증 서비스에 의하여 해당 User는 접근 제한이 된다.

DID 토큰을 받은 유저는 EMR 시스템으로 다시 한번 토큰을 통한 접근을 요청하며 EMR 시스템 내부에서 해당 토큰이 정상적인 토큰인지와 유효한 토큰인지 검증을 진행한다. 이때 검증은 Hyperledger Indy에서 진행하며 아래 [Fig 5]와 같은 과정으로 진행한다.

먼저 DID Token에 대하여 서명 인증을 진행한다[14]. DID Token은 발급자에 의하여 서명되어 있으며, 검증 과정에서 해당 토큰의 서명을 확인하고 유효성을 검증한다.



[Fig. 5] DID Token verification procedure

두 번째로 공개키 검증이 이루어지는데 DID Token은 발급된 DID와 공개키를 포함하고 있다[15].

이를 통하여 토큰이 정당한 발급자에 의해 발급되었음을 확인할 수 있다.

마지막으로 신뢰 위임 검증에 대한 절차가 이루어진다. Hyperledger Indy는 분산된 신뢰 위임 시스템을 기반이며 검증 과정에서는 토큰에 포함된 DID와 연결된 신뢰 위임 구조를 확인하여 발급자에 대한 신뢰성을 검증한다.

이를 통하여 토큰이 신뢰할 수 있는 발급자에 의해 발급되었음을 확인할 수 있다.

위와 같은 순차적인 방식으로 DID Token에 대하여 검증하며 만약 유효한 토큰일 경우 EMR System에서는 User Group에 속하는 User에게 EMR 데이터를 제공하고 만약 DID Token이 유효하지 않다면 EMR 데이터를 제공하지 않는다.

해당 시스템이 위의 시나리오 대로 구성된다면 사용자는 본인이 포함된 User Group에 맞게 EMR 데이터에 안전하고 투명하게 접근할 수 있으며 개인 의료 기록이 안전하게 관리될 수 있다.

4. 결론

본 연구에서 제안한 시스템은 Hyperledger Indy의 분산 신원 관리 기술을 기반으로 하여 각 주체 간의 안전하고 효율적인 데이터 교환을 실현한다. 이를 통해 의료 데이터의 무결성과 개인정보 보호를 동시에 보장하며, 환자 중심의 의료 서비스 제공에 기여할 것으로 기대된다.

향후 연구에서는 본 연구에서 제안된 시스템의 확장 가능성과 현실 세계 의료 기관에서의 적용 가능성을 검토하고, 보다 세부적인 보안 및 개인정보 보호 정책을 고려하는 것을 필요로 한다. 이를 통해 의료 분야에서의 디지털 신원 관리와 데이터 통합이 더욱 발전될 수 있을 것이다.

REFERENCES

[1] Hyperledger Indy[Internet], https://hyperledger-indy.readthedocs.io/en/latest.

[2] ZK proofs - Panther Protocol Documentation[Internet], https://docs.pantherprotocol.io/docs/cryptographic-primitives/zero-knowledge-proofs.

[3] Welcome to Indy Plenum's documentation![Internet], https://hyperledger-indy.readthedocs.io/projects/plenum/en/latest.

[4] What is a consensus algorithm?[Internet], https://www.techtarget.com/whatis/definition/consensus-algorithm.

[5] Introduction to Public Blockchain[Internet], https://www.lcx.com/introduction-to-public-blockchain/.

[6] Byzantine fault tolerance[Internet], https://nordvpn.com/cybersecurity/glossary/byzantine-fault-tolerance/.

[7] M. Sporny, D. Longley, M. Sabadello, D. Reed, and O. Steele, C. Allen "Decentralized identifiers (DIDs) v1.0," [Internet], https://www.w3.org/TR/did-core.

[8] S. Curran, P. Bastian, D. Hardman, C. Howland, and C. Bormann, D. Wörner, D. Bluhm, K. D. Hartog "Indy DID method,"[Internet], https://hyperledger.github.io/indy-did-method/.

[9] L. C. Edmund, C. K. Ramaiah, and S. P. Gulla, "Electronic Medical Records Management Systems: An overview," DESIDOC Journal of Library & Information Technology, Vol.29, No.6, pp.3-12, 2009.

[10] Audit ledger[Internet], https://github.com/hyperledger/indy-plenum/blob/main/docs/source/audit_ledger.md.

[11] Indy SDK configuration[internet], https://hyperledger-indy.readthedocs.io/projects/sdk/en/latest/docs/configuration.html.

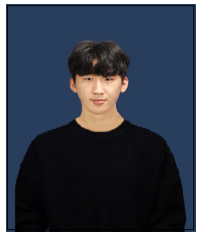
[12] Merkle Tree[Internet], https://iden3-docs.readthedocs.io/en/latest/iden3_repos/research/publications/zkproof-standards-workshop-2/merkle-tree/merkle-tree.html.

[13] Transactions[Internet], https://github.com/hyperledger/indy-node/blob/main/docs/source/transactions.md.

[14] Getting started with decentralized ID (DID) tokens[Internet], https://magic.link/docs/authentication/features/decentralized-id#token-specification.

[15] F.Muhammad, "A Review of Performance Analyzing on Public and Private Blockchain Platforms," 2020.

양 지 용(JiYong Yang) [준회원]



■ 2023년 3월 ~ 현재 : 백석대학교 컴퓨터공학부

〈관심분야〉
리눅스 커널, 시스템 보안, 블록체인

엄 효 상(Hyosang Eom) [준회원]

■ 2019년 3월 ~ 현재 : 백석대학교 컴퓨터공학부

〈관심분야〉
블록체인, 정보보안, 웹개발

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〉
이동통신 보안, 융합 보안, 개인정보보호, IoT 보안, 블록체인