https://doi.org/10.33778/kcsa.2023.23.1.063

# 보안성 강화를 위한 블록체인기술의 활용과 개선방안 연구★

유 승 재*

**요약**

본 연구에서는 블록체인 프로토콜과 네트워크 보안에 관련해서 MITM공격 및 DoS/DDoS 공격 등에 강한 대응수준을 갖출 수 있도록 블록체인 구성과 스마트 컨트랙트 상의 암호화 키 관리 방안과 에 대해 연구한다. 암호화 통신 프로토콜과 인증강화를 통한 중간자 공격(MITM)등의 데이터보안 위협에 대응, 노드간의 로드밸런싱과 분산화 된 방식으로 DDoS 공격 대응, 안전한 코딩과 취약점 검사, 안전한 합의알고리즘에 의한 스마트 컨트랙트 보안 강화, 사용자 인증과 권한 부여 강화를 통한 액세스 제어 및 인증, 블록체인 코어 및 노드의 보안성 강화, 기타 블록체인 프로토콜 업데이트 및 보안 강화를 위한 모니터링 시스템 구축 등을 통해 보안성이 강화된 블록체인 기술을 활용할 수 있을 것으로 기대된다.

# A Study on Security Enhancement for the Use and Improvement of Blockchain Technology

Seung Jae Yoo*

**ABSTRACT**

In this study, in relation to blockchain protocol and network security, we study the configuration of blockchain and encryption key management methods on smart contracts so that we can have a strong level of response to MITM attacks and DoS/DDoS attacks. It is expected that the use of blockchain technology with enhanced security can be activated through respond to data security threats such as MITM through encryption communication protocols and enhanced authentication, node load balancing and distributed DDoS attack response, secure coding and vulnerability scanning, strengthen smart contract security with secure consensus algorithms, access control and authentication through enhanced user authentication and authorization, strengthen the security of cores and nodes, and monitoring system to update other blockchain protocols and enhance security.

**Key words : Blockchain, Data security, DDoS, network security, vulnerability**

접수일(2023년 02월 22일), 수정일(2023년 03월 22일), 게재확정일(2023년 03월 31일)

★ 이 논문은 2022년도 중부대학교 학술연구비 지원에 의하여 이루어진 것임

* 중부대학교 정보보호학과 교수

# 1. 서론

COVID19 팬데믹 등 불확실성 확산으로 인하여 기업은 디지털 전환 , 공급망 탄력성 및 비즈니스 지속가능성 가속화를 위해 많은 관리적, 기술적 방안을 강구하여 왔는데, 그 대표적인 사례가 블록체인 기술의 도입이라 할 수 있다. 블록체인은 분산 컴퓨팅 기술 기반의 탈중앙성, 투명성, 불변성, 가용성을 그 특성으로 하는 데이터 위변조 방지 기술이라 할 수 있다.

블록체인 기술은 불가분 관계의 암호화폐 외에도 향상된 보안, 더 큰 투명성 및 즉각적인 추적 가능성 제공의 특성으로 금융 서비스, 공급망 및 공공 부문에서 다양한 응용 프로그램으로 활용되고 있다. IDG 보고서 'World Blockchain Spending Guide'에 따르면 블록체인 솔루션 부문에 대한 전 세계 지출은 2020년 45억 달러에서 2024년까지 190억 달러에 이를 것으로 예상되는 등 많은 부문과 영역에서 그 수요가 증대되고 있다. 또한 금융서비스 부문에서 안전한 투자운용이나 무역금융, 공공영역에서의 투명한 예산편성이나 디지털투표, IoT 부문에서 스마트 어플리케이션이나 IoT모니터링 그리고 개인 신원보호 부문에서의 디지털 ID 등 수많은 부문과 영역에서 보안성을 높이는 중요한 역할을 하고 있다.[3, 7]

IITP보고서 'ICT R&D 기술로드맵 2025'[5]에는 (그림 1)과 같이 세계 블록체인 분야의 시장규모가 2025년까지 복합연간성장률(CAGR) 69.64%로 2025년에는 390억 달러를 상회할 것으로 전망하고 있다.

(단위 : 세계시장 백만 달러, 국내시장 십억 원)

| 구분 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | CAGR |
|---|---|---|---|---|---|---|---|---|---|
| 세계 | 1,121 | 1,650 | 2,480 | 4,460 | 6,690 | 18,730 | 26,220 | 39,330 | 69.64% |
| 국내 | 27 | 40 | 60 | 107 | 161 | 450 | 629 | 944 | 69.64% |

(그림 1) 블록체인분야 시장 규모예측[5]

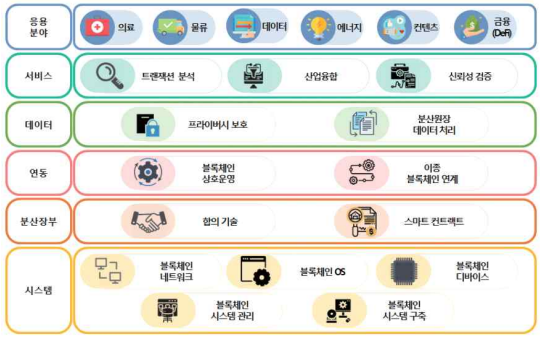
블록체인은 분산처리와 암호화 기술을 동시에 적용하여 높은 보안성을 확보하는 한 편 거래과정의 신속성과 투명성을 특징으로 한다. 이러한 블록체인 기술의 선택과 도입적용의 배경은 탈중앙화와 분산처리 방식에 대한 기본적인 안전성의 신뢰에 있다고 할 수 있다. 그러나 그동안 블록체인에 대한 여러 해킹시도와 피해사례를 볼 때 블록체인 플랫폼 응용 및 적용상의 위협요인과 구조적 측면과 기술적 측면에서 적지 않은 취약점이 있어 보안의 필요성이 대두되고 있다.[6]

본 연구에서는 블록체인 프로토콜과 네트워크 보안에 기반해서 네트워크상의 전송 데이터가 MITM공격 및 DoS/DDoS 공격에 강한 대응수준을 갖출 수 있도록 하는 블록체인 구성에 대해 살펴본다. 또한 스마트 컨트랙트 상의 암호화 키 관리 방안 등을 연구한다.

# 2. 블록체인 개념 및 구성기술

## 2.1 블록체인 구성 및 기술 요소

블록체인의 구성요소로는 분산(탈중앙화decentralization), 합의모델(consensus model), 투명성 및 개인정보보호(transparency and privacy), ID 및 액세스(identity and access control), 오픈소스(open source) 그리고 익명화(anonymization) 등으로 형성된다고 볼 수 있으며[1], 아래 (그림 2)는 블록체인의 응용영역 등의 분야 개념을 도식화 한 것이다.




(그림 2) 블록체인 분야개념도[5]

우리나라의 블록체인 기술발전 단계는 2009년부터 지원기술(blockchain-enabling technologies)단계와 블록체인 유도솔루션(Blockchain-inspired Solutions) 단계를 거쳐 스마트 계약과 탈중앙화를 통해 토큰화가 가능하고, 새로운 형태의 가치(예: 새로운 자산유형)로 거래를 가능케 하는 블록체인 완비솔루션단계(Blockchain-complete Solutions)이며 2025년 이후는 IoT, AI, SSI(Self-Sovereign Identity, 자기주권신원)

https://doi.org/10.33778/kcsa.2023.23.1.063

와 같은 기술과 융합이 가속화되는 블록체인 강화 솔루션(Enhanced-Blockchain Solutions)단계로 성장할 것으로 분석하고 있다.[5]

### 2.2 보안성 강화를 위한 블록체인 기술 활용

블록체인 기술은 공개된 분산 원장을 기반으로 하여 중앙화된 시스템과는 다른 보안성을 가지고 있기 때문에 다양한 분야에서 다음과 같이 보안성 강화 도구로 활용되고 있다.

- 보안 로깅 시스템 : 로그 데이터에 대한 위변조 방지와 무결성 보호를 블록체인 기술을 이용하여 로깅 시스템을 구축
- 사이버 보안 관리 : 보안 인증 및 접근 제어를 강화(실시간 정보공유 및 보안 취약점과 위협에 대한 신속한 대응)하여 불법적인 시스템 접근 및 해킹을 방지할 수 있는 분산화된 사이버 보안 관리 시스템을 구축
- 물류 보안 관리 : 물류 과정에서 데이터를 투명하게 기록하고, 위·변조 및 분실 방지를 위한 물류 관리 시스템 구축
- 인증서 발급 및 관리 : 인증서 정보 분산 저장하고, 해당 정보의 무결성 보장하는 인증서 발급 및 관리 시스템 구축
- 보안 검증 시스템 : 소프트웨어나 하드웨어의 보안 취약점을 검증결과를 분산 저장하고, 검증 결과의 무결성과 신뢰성을 보장할 수 있는 보안 검증 시스템을 구축
- 클라우드 보안 : 클라우드 서비스 이벤트의 실시간으로 기록 및 모니터링으로 보안 위협 사전 예방
- 개인정보 보호 : 개인정보를 암호화 및 분산저장으로 보안성 강화
- 기타 IoT 디바이스에 대한 위협대응과 지능형 보안솔루션 개발 등에 적용함으로써 보안취약점 대응 및 데이터 무결성을 보장 등의 보안 강화 기술로 활용되고 있다.

## 3. 블록체인 취약점 및 보안이슈

### 3.1 블록체인 공격사례 및 취약점

블록체인은 분산 네트워크를 기반으로 하여 거래 내용을 불변적으로 기록하는 기술로서 고도의 보안성을 가진다 할 수 있다. 하지만 플랫폼 응용 및 적용상의 취약점으로 인해 이에 대한 공격의 사례가 끊이지 않고 발생하고 있다. 언론보도를 통해 발표된 그 대표적인 사례로

2017년 발생한 'Parity 월렛 해킹 사건'은 이더리움의 스마트 계약을 통해 이루어진 해킹으로, 해커는 블록체인 내부의 스마트 계약 코드에 취약점이 있음을 이용하여 Parity 월렛에서 약 15만 개의 이더리움을 탈취했다. 2019년 발생한 'Binance 거래소 해킹 사건'은 중앙집중형 거래소인 바이낸스에서 발생한 해킹으로, 해커는 API키와 다른 정보를 이용하여 거래소에서 약 7,000 BTC를 탈취했다. 또한 2020년 발생한 'KuCoin 거래소 해킹 사건'은 또 다른 중앙집중형 거래소인 쿠코인 내부의 시스템과 API를 이용하여 다양한 암호화폐를 탈취했다.

이러한 해킹사례들은 블록체인 시스템의 취약점으로 언급된 51% 공격, 스마트 계약 취약점, 인위적인 블록 생성, DDoS 공격 뿐만아니라 블록체인 생태계의 거버넌스 구조가 미약한 점을 이용한 공격이라 할 수 있다. 아울러 암호화폐 공격의 대부분은 블록체인의 핵심기술을 대상으로 하기보다는 보안이 취약한 거래소와 전자 지갑, 그리고 지갑을 적절히 보호하지 않는 개인과 기업을 표적으로 한다. 또한 암호화폐 트랜잭션을 자신의 지갑으로 전환하기 위해 MITM공격을 시도한다.[8, 9]

이와 같이 새로운 공격기술과 방법으로 블록체인의 보안성은 끊임없이 위협을 받고 있기에, 지속적인 보안 취약점의 분석 및 대응기술 개발이 요구된다.

### 3.2 블록체인 취약점 및 보안이슈

블록체인은 탈중앙화된 분산 시스템으로서 블록체인에 저장된 모든 거래는 암호화되어 있으며, 블록체인 전체의 내용이 변경되려면 해당 블록 이후의 모든 블록을 수정해야 하므로 수정이 매우 어렵다. 그러나 이러한 블록체인 시스템의 분산형 구조는 동시에 개인정보유출의 위험성을 내포한다.

그동안 블록체인 기술에 대해 취약점의 원인을 파악하고 그에 대한 해결방안으로 다양한 보안 기술과 매커니즘이 제안되고 개발되고 있다. 예를 들어 51%

공격 방어를 위한 지연된 작업증명(delayed Proof of Work)[4]방법이나 Fork저항 알고리즘 등의 제안, 그리고 스마트 계약 보안 취약점을 줄이기 위해 다양한 코드 리뷰 및 정적분석 도구를 개발하고 있다. 또한, 거래소 등 중앙집중형 시스템의 취약점을 보완하기 위해 분산화된 시스템으로의 전환 등이 고려되고 있다. 블록체인의 안전한 응용과 적용을 위해서 현실적으로 요구되는 기술적 · 운영적 측면의 보안이슈를 살펴보면 다음과 같다.

- 개인정보보호 : 분산형 저장에 따라 데이터 무결성 강점과 동시에 유출의 위험성 내포
- 51% 공격: 강력한 컴퓨팅파워로 블록체인 네트워크에서 전체 노드의 과반수이상을 차지한 공격자는 임의로 거래 검증 및 변조 가능
- 스마트 컨트랙트 취약점 : 스마트 컨트랙트 프로그램 코드가 취약할 경우, 블록체인 시스템에서 계약 조건을 조작하거나 계약에서 보안상의 결함 악용 우려
- 인위적인 블록 생성 : 블록체인 분기 현상 유발로 공격자는 인위적으로 블록을 생성하거나 블록체인을 수정하여 이중 지불 공격 가능성
- DDoS 공격: 분산 시스템에 과도한 트래픽을 일으키는 DDoS 공격에 의해 블록체인의 정상적인 운영 방해
- 키(key) 관리 : 계정의 소유권과 거래인증의 핵심인 키의 노출은 계정에 대한 제어권한 상실로 이어지므로 엄격한 키 저장 및 관리 프로세스 필요
- 플랫폼 취약성 : 구조적 한계 또는 관리부실에 의한 비정상적 블록체인 플랫폼(중앙화된 구조, 버전 노후화 등)의 경우 탈중앙화 장점상실 및 보안취약성 노출
- 합법성 : 블록체인 기술 적용 서비스에 요구되는 정책 및 법적규정의 준수 의무

이러한 취약점은 블록체인 기술의 본질적인 한계로 인해 발생할 수 있다.

# 4. 블록체인 보안강화 방안

## 4.1 블록체인 보안취약점 분석도구

스마트 컨트랙트의 보안이 강조되면서 이더리움은 스마트 컨트랙트를 제작할 때 기본적으로 제공되는 동적 테스팅 도구인 Truffle Framework를 비롯하여 취약점 탐지성능이 더 강화된 많은 탐지도구들이 개발되고 사용되고 있다.[2] 이러한 블록체인 보안 취약점 분석 및 점검 도구<표1>를 이용하여 블록체인 기술에서 발생할 수 있는 보안 취약점을 찾아내고, 이에 대한 대응방안을 마련할 수 있다.

<표 1> 블록체인 보안 취약점 분석 및 점검 도구

| 구분 | 기능 |
|---|---|
| Certik | 스마트 컨트랙트의 보안성을 검증 |
| ChainSecurity | 스마트 컨트랙트 코드취약점 정적분석 및 스마트 컨트랙트의 동적 실행 결과 모니터링, Solidity/Vyper 언어 지원 |
| Ethersplay | 스마트 컨트랙트 코드의 실행 단계를 추적하여 취약점 식별 및 최적화된 스마트 컨트랙트를 작성 지원 |
| Hydra | 스마트 컨트랙트의 코드와 실행 로그를 분석으로 악성 스마트 컨트랙트, 데이터 노출, 권한 부여 취약점 탐지 |
| MythX / Sereum | 스마트 컨트랙트의 소스 코드를 분석하여 보안 취약점을 탐지 및 보안성 검증, EVM에서 실행 온라인서비스 |
| Mythril | 스마트 컨트랙트의 보안 검사에 사용되는 자동화 도구, EVM에서 실행 오픈소스 |
| Oyente | 코드에 대한 정적 분석을 수행하여 취약점 탐지 Solidity 언어를 지원, EVM에서 실행 오픈소스 |
| Securify | 스마트 컨트랙트 코드를 정적으로 분석하고 취약점을 검출,EVM에서 실행 오픈소스 |
| Manticore | 스마트 컨트랙트 코드와 바이너리 파일 분석, 동적 분석 및 심볼릭 실행으로 취약점 식별, EVM에서 실행 오픈소스 |
| Echidna | 시나리오 이용한 스마트 컨트랙트의 검증 |
| Truffle | 스마트 컨트랙트의 개발, 배포 테스트를 지원, 스마트 컨트랙트의 보안 취약점 사전 탐지 |
| Solidity | 개발자가 스마트 컨트랙트의 보안성을 높이기 위한 다양한 기술 적용용이 |
| Zeppelin | 스마트 컨트랙트의 개발, 배포 및 테스트를 지원하며, 보안 취약점 분석 기능 |

## 4.2 블록체인 기술 보안 및 확장성 강화 방안

블록체인과 상호작용하는 구성 요소는 코드로 작성되며 대부분의 소프트웨어 코드에는 버그와 취약점이 있다. 즉 블록체인과 상호 작용하는 전자 지갑, 스마

https://doi.org/10.33778/kcsa.2023.23.1.063

트 컨트렉트, 거래소 등 대부분의 소프트웨어가 안전하다고 볼 수는 없고, 이로 인해 트랜잭션의 안전에 위협이 되는 요소들에 대한 검토와 대응이 필요하다.

블록체인 사용자 스스로 취할 수 있는 기본적인 보안 조치(개인 키 관리, 인증 및 개인정보관리 등)는 물론 블록체인과 상호작용하는 소프트웨어 개발단계에서의 코드보안이 강조된다.

(블록체인 기술의 보안 강화 방안)

- 스마트 계약 보안 : 안전하고 신뢰성 높은 거래를 위해 취약점을 식별 및 대응, 정기적인 보안 검토 및 업데이트가 필요, 안전한 스마트 계약의 코딩 규칙과 디자인 패턴을 유지 필요
- 암호화폐 지갑 보안 : 암호화폐 지갑의 개인키를 탈취 등의 취약점에 대응하여 지갑을 하드웨어로 구현, 다중서명(multi-signature) 방식을 적용, KMaaS (Key Management as a Service) 등 암호화폐 지갑의 보안 강화 요구
- 블록체인 네트워크 보안 : 51%공격, DDoS공격 등에 대응하는 강화된 보안도구나 인증방식 도입 요구
- 블록체인 기술의 표준화: 서로 다른 블록체인 플랫폼 간의 연결성, 상호운용성 및 보안성 강화를 위해 블록체인 기술의 표준화 요구
- 블록체인 데이터 보안 강화 : 블록체인 외부에서 발생하는 위변조 공격에 대응하여 보안성 강화된 암호기술 적용 등 블록체인 데이터의 안전성 강화 방안 요구
- 라우팅 알고리즘 강화 : 카뎀리아(Kademlia)알고리즘 등 노드간의 안전하고 원활한 데이터전송을 위한 최적 경로기술 강화
- 분산해시테이블 : 트랜잭션 및 블록 데이터 저장 · 검색의 효율성, 무결성, 안전성 강화

(블록체인 확장성 및 활용 개선 방안)

- 블록체인 플랫폼의 보안 인증 : 사용자의 안전한 환경 제공을 위해 블록체인 플랫폼의 보안 인증기준과 절차 정의 및 이에 기반한 보안 인증
- 블록체인 기술의 다양한 활용 : 블록체인 기술을 이용하여 빅데이터 보안, IoT 보안, 클라우드 보안 등의 문제 해결
- 블록체인의 확장성과 성능향상 : 샤딩(sharding)을 이용하여 각각의 블록체인의 데이터 동기화를 빠르게 수행하고 블록체인 데이터 처리 속도 향상
- 개인정보 보호 : 블록체인 상의 개인정보보호를 위한 데이터 익명화 기술 적용
- 법적 문제 해결: 스마트 컨트랙트의 법적 효력, 블록체인 상의 데이터가 법적 증거 등 블록체인 기술에 대한 국내외 법적인 규제 및 정책 확립
- 기타 체계화된 블록체인 기술의 교육 및 보안 인식 제고 프로그램 개발

(블록체인 프로토콜과 네트워크 보안을 강화)

- 암호화된 통신 프로토콜 : 중간자 공격(MITM)과 같은 보안 위협으로부터 데이터를 보호
- 분산화된 DDoS 방어 시스템 : 캡차(CAPTCHA) 등 인증강화, 노드간의 로드 밸런싱과 분산화된 DDoS 공격대응시스템
- 보안 강화를 위한 블록체인 프로토콜 업데이트 : 새로운 기술과 보안 취약점에 대한 대응
- 노드 보안 강화 : 보안운영체제와 보안소프트웨어, 방화벽, 취약점 검사 등을 통한 노드 보안성 강화
- 스마트컨트랙트 보안강화 : 안전한 코딩과 취약점 검사, Proof of Work(PoW), Proof of Stake(PoS), Delegated Proof of Stake(DPoS) 강화
- 엑세스 제어 및 인증 : 사용자인증과 권한부여 등의 엑세스 제어 강화 및 블록체인 네트워크 노드간 신뢰통신 강화
- 블록체인 코어의 보안성 강화 : 취약점 진단 및 공격차단 강화로 블록체인네트워크 핵심기술의 보안성을 강화
- 보안 강화를 위한 모니터링 시스템 구축 : 블록체인 네트워크 상태 실시간 모니터링 및 신속한 보안위협대응체제 구축

블록체인의 불변성 속성으로 데이터의 생성 기록 및 변경 이력까지 제공함으로써 데이터 투명성에 대한 장점을 갖지만, 개인정보와 같이 잊힐 권리(right to be forgotten)에 대한 문제, 삭제가 불가능한 환경에서 사이즈가 큰 데이터들을 분산 원장으로 다루는 비효율성 문제 등은 블록체인의 구조적인 난제이지만,

이상의 점검항목을 반영한 블록체인 프레임을 구성한다면 블록체인 프로토콜과 네트워크 보안을 강화됨으로써 MITM 공격 및 DoS/DDoS 공격 등의 각종 보안 위협으로부터 블록체인 플랫폼의 효과적인 보호가 이루어 질 것으로 기대된다.

## 5. 결론

블록체인 기술은 기존의 중앙집중형 시스템과는 달리 분산형 시스템으로, 거래 내역을 공유하고 기록하는 기술이다. 그러나 블록체인 기술도 보안 취약점과 위협에 노출될 수 있으므로 이러한 취약점과 위협에 대한 대응은 블록체인 기술의 발전과 보안을 강화하는 데 필수적이다. 앞에서 블록체인 기술의 보안 취약점과 보안이슈 등을 조사하고 블록체인 기술의 보안 강화 방안을 제시하였다.

암호화 통신 프로토콜과 인증강화를 통한 중간자 공격(MITM)등의 데이터보안 위협에 대응, 노드간의 로드밸런싱과 분산화된 방식으로 DDoS 공격 대응, 안전한 코딩과 취약점 검사, 안전한 합의알고리즘에 의한 스마트 컨트랙트 보안 강화, 사용자 인증과 권한 부여 강화를 통한 엑세스 제어 및 인증, 블록체인 코어 밑 노드의 보안성 강화, 기타 블록체인 프로토콜 업데이트 및 보안 강화를 위한 모니터링 시스템 구축 등을 통해 보안성이 강화된 블록체인 기술을 활용할 수 있을 것으로 판단된다.

이는 블록체인 응용 및 서비스 플랫폼에 있어서 기반기술의 개선, 연속성 있는 신뢰 네트워크 확보 및 다양한 서비스의 완전성과 신뢰성 증대로 이어져 블록체인 기술의 발전과 함께 기업 및 개인의 안전한 거래를 지원함으로써 산업과 경제발전에 크게 기여할 것으로 기대된다.

## 참고문헌

[1] S. SINGH 외2인 , “Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network” SPECIAL SECTION ON INTERNET-OF-THINGS ATTACKS AND DEFENSES: RECENT ADVANCES AND CHALLENGES Vol.2, IEEE, 2021.

[2] 방지원 외1인, “스마트 컨트랙트 취약점 탐지 도구 동향 분석” KNOM Review, Vol.25 No.01, pp.49-61, 2022.

[3] 지승원 외6인, “블록체인기반의 SCADA시스템 보안”, 융합보안논문지 제19권제5호 pp55-61, 2019.

[4] 김인영 외 2인, “51% 공격에 저항 가능한 신규합의 알고리즘”, 추계학술대회발표논문집, 제25권 제2호, pp.288-291, 한국정보처리학회, 2018.

[5] ICT R&D 기술로드맵 2025 차세대보안 · 블록체인 IITP

[6] 전자금융과 금융보안, 제28호, 금융보안원, 2022.

[7] Cem Dilmegani, “Top 17 Blockchain Applications & Use Cases in 2023”, AI Multiple.

[8] 김미희, “블록체인시대의 보안위협과 대응방안”, 이글루보안이슈, 2019.

[9] IDG Deep Dive, “블록체인을 둘러싼 보안 위협과 과제” 2018.

## 〔저자소개〕

유 승 재 (Seung-Jae Yoo)
1988년 2월 동국대학교 이학사
1990년 2월 동국대학교 이학석사
1998년 2월 동국대학교 이학박사
1997년 3월 ~ 현재 중부대학교 정보보호학과 교수
email : sjyoo@joongbu.ac.kr