사이버 공격 대응을 위한 블록체인 기반 침해지표 정보 생성 및 공유 메커니즘

이형우*
한신대학교 AISW대학 교수

Blockchain Based IoC(Indicators of Compromise) Generation and Sharing Mechanism for Cyber Attack Response

Hyung-Woo Lee*
Professor, School of Computing and Artificial Intelligence, Hanshin University

요 약 최근 사이버 공격이 급증함에 따라 능동적 대응 체계 구축이 필요하다. 본 연구에서는 사이버 공격 발생 시 생성되는 침해지표(Indicators of Compromise : IoC) 정보를 블록체인(Blockchain) 시스템에 저장/관리토록 하여 사이버 공격에 관한 위협 정보를 효율적으로 공유할 수 있는 메커니즘을 제시하였다. 제안된 메커니즘은 다이아몬드 모델 기반으로 생성된 IoC 정보를 분산형 블록체인 시스템 내에 저장하여 IoC 정보에 대한 위·변조를 방지하고 사이버 위협 정보 공유 과정에서의 신뢰도를 향상시켰다. 제안한 메커니즘을 이용할 경우 기존의 중앙 집중형 또는 MISP 기반의 IoC 공유 방식 보다 보안성, 실시간성 및 위협 정보 공유 시 우수한 성능을 제공하므로, 이를 통해 조직 간 위협 인텔리전스 협업 체계를 강화하고 더욱 향상된 사이버 공격 탐지 및 대응 체계를 수립할 수 있다.

주제어 : 사이버 공격, 침해지표, 블록체인, 위협 정보 공유, 침해지표 구조, 공유 모델

Abstract In view of the recent proliferation of cyber attacks, it is essential to establish a proactive and systematic framework for effective cyber threat response. This study introduces a formalized mechanism designed to facilitate the reliable generation and secure sharing of Indicators of Compromise (IoCs) through the integration of blockchain technology. The proposed mechanism employs a diamond model-based structure to define IoC information and utilizes a distributed blockchain infrastructure to ensure immutability, traceability, and resistance to tampering. By enabling real-time validation and secure dissemination of threat indicators, the framework significantly addresses the limitations inherent in traditional centralized and MISP-based sharing models. Consequently, the proposed system enhances the integrity, responsiveness, and interoperability of cyber threat intelligence sharing, thereby contributing to the establishment of a robust and collaborative cyber defense architecture among participating entities.

Key Words : Cyber Attack, Indicators of Compromise, Blockchain, Threat Sharing, IoC Structure, Sharing Model

이 논문은 한신대학교 학술연구비 지원에 의해 연구되었음.
*교신저자 : 이형우(hwlee@hs.ac.kr)
접수일 2025년 07월 12일 수정일 2025년 08월 04일 심사완료일 2025년 08월 14일

1. 서론

최근 들어 사이버 공격이 급증하고 있으며 그림 1과 같이 점차 지능화, 고도화되고 있다. 특히 랜섬웨어, 공급망 공격(Supply Chain Attack), 사회공학기반 침입, APT(Advanced Persistent Threat)와 같은 공격을 통해 기존의 방어 체계를 우회하거나 무력화시키는 사례가 증가하고 있다. 이에 따라 침해 사고 발생 이후 과정에서의 대응 뿐만아니라, 지능화된 사이버 침해 사고 발생 이전 단계에서 공격에 대한 탐지 및 예방, 실시간 모니터링을 위한 시스템 구축이 필요하다[1].

침해지표(Indicators of Compromise: IoC)는 사이버 공격이 발생하였을 경우 또는 현재 진행중에 있을 경우 이를 표시하는 디지털 포렌식 증거이다[2-5]. 이는 보안 로그, 악성코드 해시값, 도메인 주소, IP 주소, 행위 기반 징후 등과 같이 다양한 형태로 존재하며 이와 같은 IoC 정보를 통해 사이버 공격의 흔적을 포착하고 동일 유형의 공격 확산을 방지할 수 있으므로, 신속하고 정확한 IoC의 수집, 분석, 공유는 사이버 보안에서 매우 중요한 요소이다. 정부 및 공공기관/기업에서는 IoC를 활용하여 실시간 보안 감시, 침해 사고 대응(Incident Response: IR), 보안 위협 인텔리전스(Threat Intelligence : TI), 디지털 포렌식 조사 분석 과정 등을 수행할 수 있다. 따라서 IoC를 이용하여 네트워크 트래픽, 로그 및 파일 등에 대한 이상 징후를 감지할 수 있으며, 침해사고 발생 가능성을 사전에 파악할 수 있고, 사고 발생 후 원인을 추적하고 대응 방안을 마련하는 과정에 활용하거나 조직 간 IoC 정보를 공유하여 대단위 사이버 공격에 공동 대응할 수 있는 장점을 제공한다[6-8].

[Fig. 1] Types of Cyber Attacks

그러나 현재까지의 IoC 공유 메커니즘은 주로 중앙집중형 구조에 의존하고 있다. 국가 또는 기관 차원에서 운영되는 MISP(Malware Information Sharing Platform)[9], TAXII(Trusted Automated eXchange of Indicator Information)[10] 등을 사용하여 관리 효율성과 일관성을 제공하지만, 단일 실패 지점(Single Point of Failure)의 위험, 정보 위·변조 가능성 및 실시간성 부족 등의 한계를 내포하고 있으며, 이기종 보안 시스템 간 상호 운용성이 부족하며 데이터에 대한 신뢰성 검증이 어렵다는 문제점이 발견되고 있다.

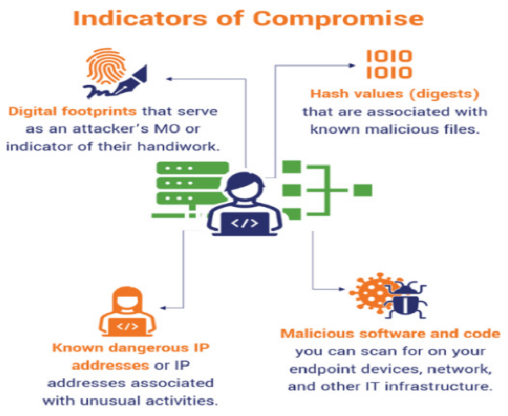
이에 본 연구에서는 블록체인 기술의 분산형 저장 및 위변조 방지 특성을 활용하여 사이버 공격 발생시 생성되는 IoC 정보에 대한 신뢰성과 무결성을 제공하고, 실시간 공유가 가능하도록 새로운 IoC 생성 및 공유 메커니즘을 제안하였다. 특히 다이아몬드 모델을 기반으로 한 침해지표 구조로 정형화하여 IoC 표현의 일관성과 분석 용이성을 확보하며, Hyperledger Fabric 등과 같은 프라이빗 블록체인 구조를 이용하여 민감한 보안 데이터를 안전하게 관리할 수 있다. 이를 통해 기존 침해지표 공유 체계의 문제점을 해결하고, 향후 사이버 위협 인텔리전스 시스템의 발전 방향을 제시하고자 한다.

2. 침해지표(IoC) 기반 사이버 공격 대응

2.1 기존 침해지표 공유 기법

최근 사이버 위협 인텔리전스(Cyber Threat Intelligence: CTI) 시스템을 이용한 사이버 위협 정보 공유에 대한 관심이 증가함에 따라 침해지표(IoC) 정보를 다양한 시스템 간에 효과적으로 공유하고자 하는 연구가 활발히 진행되고 있다. 그림 2와 같이 침해지표는 사이버 공격 또는 보안 침해 사건이 발생했음을 나타내는 디지털 증거 자료에 해당하는 것으로 보안 운영 센터(SOC), 침해사고 대응팀(Computer Emergency Response Team: CERT), 포렌식 전문가 등에 의해 분석을 통해 사이버 공격에 대한 사전 예방, 실시간 탐지 및 사후 대응의 핵심 정보로 활용된다.

현재까지 가장 널리 사용되는 위협 정보 공유 시스템으로는 MISP와 STIX(Structured Threat Information Expression)[11]/TAXII 프로토콜 기반 시스템이 있으며, 이들은 IoC의 수집, 표현, 전송, 공유의 전 과정을 구조화된 방식으로 지원한다. 그러나 이러한 시스템은 중앙 집중형 구조를 기반으로 하고 있어 단일 실패 지점(Single Point of Failure: SPOF), 위·변조 가능성, 그리고 보안성 및 확장성 측면에서의 한계를 내포하고 있다.



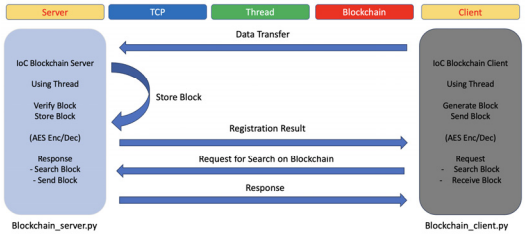
[Fig. 2] Indicators of Compromise

기존의 IoC 공유 방식으로는 대표적으로 MISP와 STIX/TAXII 메커니즘을 이용한 중앙 집중형 모델에 의존하고 있다. MISP는 다양한 형태의 IoC 정보를 JSON 기반으로 표현하여 공유할 수 있는 플랫폼으로, 유럽을 중심으로 다수의 정부기관 및 기업에서 활용되고 있다[5]. 국가 기관, 공공기관, 금융권 및 기업간 IoC 실시간 공유 기능을 제공하며 MISP 플랫폼을 기반으로 보안 커뮤니티 운영 등이 가능하다는 장점이 있으나, 각 기관마다 상이한 구조와 형태로 개발되어 있어 이에 대한 개선 과정이 필요하다.

MISP는 사용자 친화적인 웹 UI와 RESTful API를 통해 IoC 등록, 검색, 필터링, 통계 기능 등을 제공한다. 그러나 시스템의 중앙 집중 구조로 인해 단일 실패 지점(SPOF)에 취약하며, 외부 공격이나 오작동 발생 시 전체 시스템의 운영에 영향을 미칠 수 있다. 또한 STIX[11]는 사이버 위협 정보 표현 언어로 공격자 TTP(전술·기술·절차), 피해자 정보, 인프라 정보 등을 구조화된 형식으로 표현할 수 있다. TAXII(Trusted Automated Exchange of Indicator Information)[10]는 STIX 데이터를 자동 전송하기 위한 전송 프로토콜로, JSON 기반 메시지 형식을 사용하며, pull/push 방식의 데이터 동기화를 지원한다. 그러나 STIX/TAXII는 구조가 매우 복잡하여 IoC 생성 및 변환 과정에서 기술적 부담이 크고, 실시간 검증이나 위변조 방지 기능이 내재되어 있지 않다[3][7]. 따라서 최근 급증하고 있는 사이버 위협 정보를 효율적으로 공유할 수 있는 메커니즘이 필요하다.

2.3 블록체인 기반 침해지표 공유 방식

침해지표(IoC)는 사이버 공격이 발생했을 경우 이를 표현하는 세 가지 방식을 사용할 수 있다. 첫째, 비구조화된 텍스트 기반 IoC인 경우 보안 리포트, 이메일, PDF 파일 등의 문서로 표현되는 방식으로 표준화되어 있지 않아서 자동화 처리 과정에 어려움이 존재한다는 문제점이 있다. 이를 개선하기 위해 CSV, JSON 및 XML 등과 같은 구조화된 파일 포맷 형태로 침해사고 발생 정보를 표현하는 방법이 있다. 이 경우 데이터 처리와 자동화 과정이 상대적으로 용이하며 보안 시스템간 연동이 가능하다는 장점이 있다. 이때 가장 중요한 것 중 하나는, 사이버 공격 발생시 위협 정보를 IoC로 표현한 후 이를 효율적으로 공유 및 전파할 수 있는 방법이 필요하다.



[Fig. 3] Blockchain based IoC Data Sharing

그림 3과 같이 블록체인(Blockchain) 기반 IoC 공유 기술[12-15]은 기존 MISP 등과 같은 중앙 집중형 모델의 한계를 극복하고 위협 인텔리전스 공유의 신뢰성과 투명성을 강화하는 방법이다. 블록체인은 모든 참여자가 동일한 데이터를 보유하는 분산형 구조를 가지며, 한 번 기록된 정보는 변경이 불가능하다는 특성(불변성, immutability)을 갖는다. 또한 모든 기록은 시간순으로 체인 형태로 연결되어 있어, 침해지표의 생성, 검증, 공유 이력을 투명하게 추적/관리할 수 있다.

블록체인을 활용한 IoC 공유 방식은 크게 퍼블릭 블록체인(Ethereum 등)을 기반으로 한 개방형 공유 모델과, Hyperledger Fabric과 같은 프라이빗 블록체인을 기반으로 한 폐쇄형 공유 모델로 나눌 수 있다. 퍼블릭 블록체인은 누구나 접근 가능하다는 장점이 있으나, 개인정보 보호 및 접근 제어 측면에서 한계가 있다. 이에 반해 프라이빗 블록체인은 참여자 간 신뢰 관계를 기반으로 운영되며, 스마트 컨트랙트를 통해 IoC 등록·수정·검증·조회 등의 기능을 자동화할 수 있다[12-14].

실제 Hyperledger Fabric 기반 블록체인 플랫폼은 채널(Channel) 기능을 활용하여 기관 간 개별 데이터 공유를 제한할 수 있으며, 사용자 인증 및 접근 권한 관리가 용이하다. 이러한 특성은 민감한 보안 정보 공유에 있어 법적·기술적 안정성을 확보하는 데 효과적이다. 블록체인 기반 IoC 공유 시스템은 위·변조 방지뿐만 아니라,

실시간 데이터 검증 및 자동화된 교차 참조 기능을 통해 탐지 정확도를 높이고, 보안 운영 센터(SOC) 간 협업 역량을 향상시킬 수 있음이 입증되었다. 이러한 한계를 극복하기 위해 블록체인 기술을 활용하여 IoC 정보 공유 방식에 적용할 수 있다. 블록체인 기술을 활용한 IoC정보는 블록체인의 속성을 상속받음에 따라 위변조 방지 및 실시간 검증이 가능하다는 장점을 제공한다. 특히 스마트 컨트랙트(Smart Contract)를 활용하면 IoC 정보의 등록, 수정, 접근 제어, 검증 등의 과정을 자동화할 수 있으며, 블록체인에 저장된 모든 기록은 시간 순으로 영구 보존되어 사이버 공격 대응 이력의 추적성과 신뢰성을 확보할 수 있다.

따라서 블록체인을 이용할 경우 다양한 조직 간 위협 정보를 안전하게 교환하고 실시간으로 위협을 탐지 및 차단할 수 있으며, 또한 블록체인 기반 IoC 플랫폼은 서로 신뢰 관계가 부족한 조직 간에도 신뢰할 수 있는 위협 정보 공유를 가능하므로 향후 국가·산업 간 협력 기반 사이버 보안 체계의 핵심 기술로 발전 가능하다.

3. 블록체인 기반 침해지표 정보 표현 및 공유 메커니즘

3.1 블록체인 기반 침해지표 공유 방식

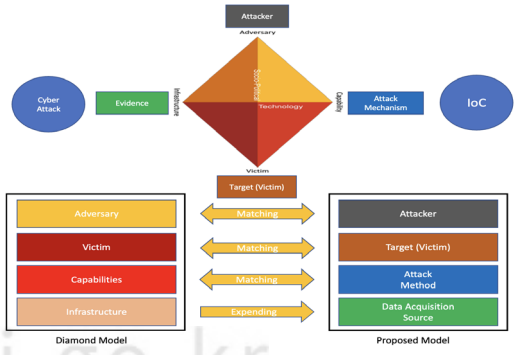
이에 본 논문에서는 아래와 같이 블록체인 기반 IoC 공유 메커니즘의 전체 흐름도를 제시하였으며 주요 구성 단계는 다음과 같다.

- IoC 생성 및 수집 단계 : 침해지표 정보는 EDR, NDR, SIEM 등의 보안 장비 또는 CTI 피드로부터 수집되며, 그림 4와 같은 Diamond 모델 기반의 분석을 통해 구조화된다.
- IoC 정규화 및 해시 처리 : 수집된 IoC는 JSON 형태로 변환된 후, 무결성 확보를 위해 SHA-512 해시값이 생성된다.
- 스마트 컨트랙트를 통한 블록체인 등록 : 정규화된 IoC는 스마트 컨트랙트를 통해 Hyperledger Fabric 블록체인에 등록된다. 이때 트랜잭션 내역은 영구 보존되며 검증 기능이 자동화된다.
- 공유 요청 및 검증 프로세스 : 타 조직이 IoC에 접근할 경우, API를 통해 조회하며 해당 데이터는 블록체인 내 해시값과 비교되어 검증된다.
- 정보 연계 및 협업 대응 : 검증된 IoC는 Threat Intelligence 플랫폼(MISP, OpenCTI 등) 또는 대응 시스템과 연계되어 협업 대응에 활용된다.

본 메커니즘은 블록체인의 불변성과 스마트 컨트랙트 기반의 자동화 기능을 결합함으로써, IoC 정보의 실시간 공유, 무결성 보장, 신뢰 검증을 동시에 만족시키는 기술적 기반을 제공한다. 본 장에서는 사이버 공격 대응을 위한 블록체인 기반 침해지표 생성 및 공유 메커니즘의 구성 요소와 동작 방식을 구체적으로 제시한다. 제안하는 메커니즘은 크게 침해지표 생성 단계, IoC 구조 정규화, 블록체인 저장 및 검증, 공유 API 기반 연계 모듈로 구성된다. 이를 통해 IoC 정보의 실시간 수집, 검증, 공유, 추적이 가능한 분산형 보안 인프라를 구현한다.

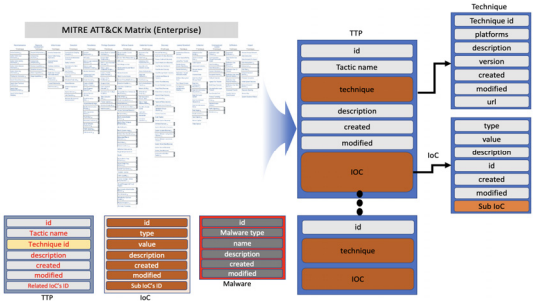
3.2 다이아몬드 모델 기반 침해지표 공유

사이버 공격 정보를 효율적으로 표현하고 이를 공유하기 위해서는 새로운 형태의 IoC 표현 구조 및 메커니즘이 필요하므로, 아래 그림 4와 같은 다이아몬드 모델(Diamond model)에 기초하여 사이버 위협에 대한 (1) 공격자(Adversary): 악성 IP, 도메인, 이메일, 해커 그룹 등, (2) 공격 기법(Capability) : 공격자가 사용하는 악성코드, 익스플로잇 도구, 무기화 기법, (3) 공격 인프라(Infrastructure) : C2 서버, 피어 투 피어 네트워크, 스크립트 호스팅 URL, 그리고 (4) 피해 대상(Victim) : 공격 대상이 된 기업, 서버, 클라이언트, 사용자 ID 등의 네 가지 핵심 요소로 분류하여 침해사고를 체계적으로 표현할 수 있다. 본 논문에서는 기존 다이아몬드 모델을 기반으로 침해사고 발생시 위협 정보를 아래와 같은 IoC 형태로 구성한다. 이와 같은 정보는 JSON 포맷의 정형 데이터로 변환되며, 이후 블록체인 저장을 위한 해시 처리 대상이 된다.



[Fig. 4] Diamond Model based IoC Representation

또한, 아래 그림 5와 같이 MITRE ATT@CK Matrix로 표현 가능한 TTP(Tatics, Technique, Procedure) 정보를 포함하며 상세 공격 인프라와 피해자에 대한 정보를 포함하여 IoC 정보를 구성할 수 있다[16].



[Fig. 5] IoC Data Format and Structure

이와 같이 생성된 침해지표에 대해서는 이기종 보안 위협 인텔리전스 시스템 간에 공유할 수 있어야 한다. 각 시스템 마다 다양한 형태의 IoC 포맷과 표현 방식이 존재하므로 (1) 데이터 수집, (2) 정규화, (3) 변환 및 (4) 공유의 4단계 침해지표 간 변환(Transformation) 과정을 통해서 다양한 보안 시스템과 연계 및 공유가 가능하다.

3.3 블록체인 기반 침해지표 공유 구조

최근 다양한 형태의 사이버 공격이 급증하고 있어 효율적 대응이 필요하다. 사이버 공격 발생시 이를 침해지표로 생성하고 공유하는 방법이 필요하다. 블록체인 시스템에 침해지표를 저장/공유할 경우 효율적인 방식으로 침해사고에 대응할 수 있으며, 기존 사이버 공격 대응 시스템에 비해 능동적 대응

체계 및 사이버 공격 발생시 정확한 분석 체계를 구축할 수 있다. 제안하는 블록체인 기반 공유 시스템은 Hyperledger Fabric 등과 같은 프라이빗 블록체인 네트워크로 구성되며, 각 보안 기관은 하나의 Peer 노드로 참여한다. 전체 아키텍처는 다음과 같은 요소로 구성된다.

- Ledger: 각 IoC 데이터의 해시값과 메타 정보를 블록 단위로 저장
- Smart Contract: IoC 등록 요청 시 유효성 검증, 중복 검사, 블록 저장 자동화
- Channel: 기관 간 별도의 접근 권한과 프라이버시를 보장하는 분리된 데이터 채널
- API Gateway: 외부 보안 솔루션(MISP, OpenCTI 등)과 연동 가능한 인터페이스

3.4 블록체인 기반 침해지표 정보 공유 메커니즘

다음은 제안된 블록체인 기반 침해지표 공유 메커니즘의 구체적인 동작 절차이다.

- IoC 데이터 수집 및 분석 : EDR, SIEM, NDR 등과 같은 조직 내부 보안 시스템 또는 외부 CTI 피드로부터 침해지표 원시 데이터를 실시간으로 수집한다. 수집된 원시 데이터는 로그, 네트워크 흐름, 이벤트 정보 등 다양한 형태로 존재하며, 이를 전처리하여 의미 있는 IoC 지표로 정제 또는 변환한다.
- 다이아몬드 모델 기반 구조화 : 수집된 지표는 다이아몬드 모델의 네 가지 구성요소(공격자, 능력, 인프라, 피해자)에 따라 분류되며, 상호 연결된 관계 기반으로 JSON 포맷으로 구조화된다. 이를 통해 IoC는 정형화된 데이터로 변환되어 표준 형태로 내부 보안 시스템 또는 외부 CTI 피드 간에 손쉽게 공유가 가능하도록 구조화된다.
- 무결성 검증을 위한 해시 생성 : 구조화된 IoC는 SHA-512 알고리즘을 사용하여 해시값을 생성하고, 이 해시값은 해당 IoC의 유일성을 식별할 수 있는 고유 정보로 활용된다. 해시 처리는 데이터의 위변조 여부를 감지하기 위한 사전 단계로, 향후 공유 및 검증 절차의 핵심 요소가 된다.
- 블록체인 저장 및 스마트 컨트랙트 실행 : 생성된 해시값과 메타데이터는 스마트 컨트랙트를 통해 블록체인 네트워크에 등록된다. 스마트 컨트랙트는 IoC 중복 여부 확인, 등록 시간 기록, 데이터 유효성 검증 등의 기능을 자동으로 수행하며, 트랜잭션은 분산 합의를 거쳐 블록에 포함된다.
- 기관 간 정보 공유 요청 및 접근 제어 : 타 조직이 IoC 정보에 접근하고자 할 경우, API 요청을 통해 해당 IoC의 해시값과 메타정보를 질의한다. 시스템은 등록된 해시값과 비교하여 무결성 여부를 실시간으로 검증하며, 승인된 기관에만 정보를 제공한다. 이 과정은 인증 및 접근 제어 정책을 통해 안전하게 제어된다.
- 공유된 IoC의 연계 활용 : 검증을 통과한 IoC 정보는 MISP, OpenCTI 등과 같은 위협 인텔리전스 시스템 또는 침입 방지 장비(IPS), 탐지 시스템(IDS), 방화벽 등과 연동되어 자동 분석 및 대응에 활용된다. 또한 공유 이력은 모두 블록체인에 기록되어 감사 추적(Audit Trail)이 가능하다.

이와 같이 본 연구에서 제시하고자 하는 메커니즘은 블록체인의 불변성과 스마트 컨트랙트 기반의 자동화 기능을 결합함으로써, IoC 정보의 수집부터 공유, 검증, 대응까지 전 주기적 위협 대응 체계를 기술적으로 실현한다. 이를 통해 정보 신뢰성을 보장함과 동시에 사이버 보안 협업의 실효성을 향상시킬 수 있다.

4. 블록체인 기반 침해지표 정보 생성 및 공유 시스템 설계 및 구현

4.1 블록체인 기반 침해지표 정보 생성 및 공유

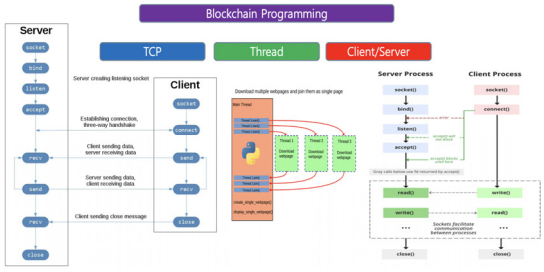
제안하는 시스템은 IoC 데이터를 생성, 정규화, 검증, 공유하는 전 과정을 자동화하고, Hyperledger Fabric 블록체인 시스템 또는 일반화된 블록체인 방식을 적용하여 위변조 방지 및 신뢰성 확보 기능을 제공하는 구조로 설계되었다. 범용성과 학습 목적을 고려하여 Python과 PyCryptodome 라이브러리를 활용한 경량 블록체인 환경 구현 방안을 제시한다. 해당 블록체인은 IoC 데이터를 블록 내에 포함하고, 무결성 검증 및 체인 구조를 단순화된 형태로 시뮬레이션할 수 있다. 이를 통해 IoC 공유 및 추적이 가능한 분산 저장 모델을 시험적으로 구현할 수 있으며, 핵심 모듈은 다음과 같이 구성된다.

- IoC 생성기 (IoC Generator) : 외부 보안 장비 또는 위협 인텔리전스 피드로부터 IoC 데이터를 수집하고, 다이아몬드 모델 기반으로 분석한 후 정규화된 JSON 포맷으로 변환
- 무결성 해시 모듈 : IoC의 해시값(SHA-256)을 생성하여 고유 식별자와 무결성 검증 용도로 사용
- 블록체인 연동기 (Blockchain Connector) : 스마트 컨트랙트 호출을 통해 IoC 정보를 블록체인에 저장하고 조회
- 스마트 컨트랙트 (Chaincode) : IoC 등록/조회/검증에 대한 비즈니스 로직 자동 실행
- RESTful API 서버 : 외부 시스템(MISP, SIEM 등)과의 연계를 위한 JSON 기반 통신 인터페이스 제공
- 시각화 및 UI 대시보드 : 공유 이력, 블록 등록 상태, 기관 간 협업 이력 등을 확인할 수 있는 인터페이스

본 연구에서 제안한 IoC 포맷 구조로 표현할 수 있도록 파이썬 언어를 이용하여 IoC 정보 표현 시스템을 설계 및 구현하였다. 구현한 시스템은 Python 3.10과 PySide6 모듈을 이용하여 GUI 프로그램을 제작하였으며 수집한 침해지표를 MISP 등의 위협정보 공유 플랫폼에 등록하는 기능을 제공한다.

4.2 시스템 설계 및 구현 상세

블록체인을 이용한 IoC 데이터 공유 시스템을 구현하기 위해 클라이언트-서버 모델 기반 TCP 접속 방식을 이용하고 다중 접속을 지원하기 위해 Thread 기반 접속 방식을 구현하였다. Python 언어를 이용하여 아래 그림 6과 같이 블록체인 방식을 이용한 IoC 데이터 공유 방식을 설계 및 구현하였다.



[Fig. 6] Client/Server based TCP MultiThread based IoC Blockchain

해당 블록체인은 IoC 데이터를 블록 내에 포함하고, 무결성 검증 및 체인 구조를 단순화된 형태로 시뮬레이션할 수 있다. 이를 통해 IoC 공유 및 추적이 가능한 분산 저장 모델을 시험적으로 구현할 수 있으며, 핵심 모듈은 다음과 같다.

- Block 클래스 : IoC 데이터를 담는 블록 구조 정의. 각 블록은 timestamp, 이전 해시, 현재 해시, IoC payload로 구성된다.
- Blockchain 클래스 : 블록 리스트로 구성된 체인 구조. 블록 추가, 유효성 검증, 체인 무결성 검사 기능 포함한다.
- Hash 생성 및 IoC 저장 모듈 : 암호화 라이브러리 PyCryptodome의 SHA-512 모듈을 활용하여 블록 및 IoC 데이터의 해시 생성과정을 수행한다.

```python
class Block:
    def __init__(self, index, previous_hash, timestamp, data):
        self.index = index
        self.previous_hash = previous_hash
        self.timestamp = timestamp
        self.data = data
        self.hash = self.calculate_hash()

    2 usages (1 dynamic)
    def calculate_hash(self):
        data = f"{self.index}{self.previous_hash}{self.timestamp}{self.data}"
        return hashlib.sha256(data.encode()).hexdigest()
```

```python
class Blockchain:
    def __init__(self):
        self.chain = [self.create_genesis_block()]
    1 usage
    def create_genesis_block(self):
        return Block( index: 0, previous_hash: "0", int(time.time()), data: "Genesis Block")
    3 usages
    def get_latest_block(self):
        return self.chain[-1]
    4 usages (2 dynamic)
    def add_block(self, new_block):
        new_block.previous_hash = self.get_latest_block().hash
        new_block.hash = new_block.calculate_hash()
        self.chain.append(new_block)
```

[Fig. 7] Internal Structure of IoC Blockchain

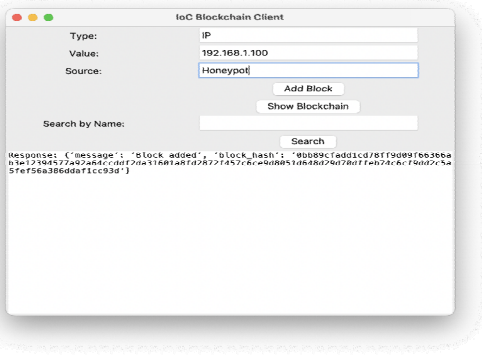
제안한 구조는 IoC 정보를 구조화하여 블록체인에 기록하고, 블록 간 연결을 통해 변경 불가능한 위협 인텔리전스 공유 구조를 모사하는 데 활용될 수 있다. 실제 환경에서는 이를 확장하여 IPFS와 연계하거나, Flask 기반 REST API를 통해 외부 공유 기능도 연동 가능하다.

- IoC Generator : 다양한 IoC 입력 포맷(CSV, JSON, STIX 등)을 수용하며, 필드 정규화, 중복 제거, 필수 항목 검증 등의 사전 처리 수행.
- Blockchain Connector : Hyperledger Fabric SDK (Python 기반)를 활용하여 스마트 컨트랙트와 직접 통신하며, 채널 구성, 트랜잭션 제출, 응답 처리 기능 포함.
- Smart Contract (Chaincode) Generator : Python 또는 Go로 작성되며, IoC() 생성, 검증 및 질의 기능을 제공한다. 신규 IoC 등록 및 타임스탬프 기록하거나, 제출된 IoC 데이터의 해시값과 블록체인 내 기존 해시 비교하고, 특정 IoC의 존재 여부 및 등록 내역 반환하는 기능을 제공한다.

4.3 IoC 블록체인 클라이언트/서버 시스템 구현 결과

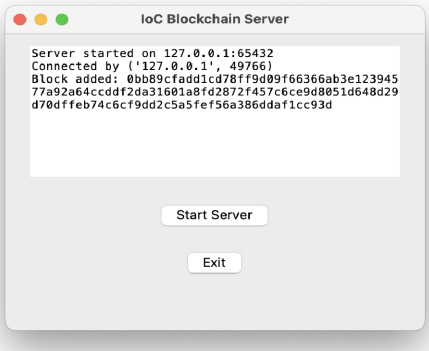
클라이언트/서버 기반 IoC 블록체인 정보 시스템 구현 결과는 다음과 같다. IoC 정보를 저장한 블록체인에 대해 등록 과정을 수행하고 저장된 블록 정보를 검색하는 과정은 다음 그림과 같다. Python 3.11 인터프리터를 이용하여 아래 그림과 같이 IoC 블록체인 서버와 클라이언트 모듈을 구현하였다. 블록체인 데이터에 대한 기밀성, 무결성 및 위변조 방지 기능을 제공하기 위해 PyCryptodome 모듈을 이용하여 AES 암복호화 과정 및 SHA-512 기반 해시값을 생성하고 이를 IoC 블록체인 내에 저장할 수 있는 시스템을 구현하였다. PyCharm IDE를 이용하였으며, TCP 소켓을 이용하여 Multi-Thread 방식으로 클라이언트/서버 모듈을 개발하였다.

아래 그림 8과 같이 IoC 블록체인 클라이언트 모듈에서는 IoC 정보를 입력하면 해당 내용은 서버로 전송되며, 서버 내 블록체인에 등록되는 구조이다.



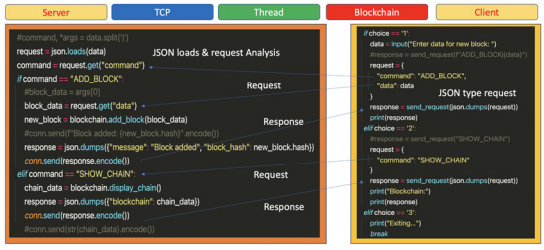
[Fig. 8] IoC Blockchain Client Module

서버 모듈에서는 그림 9와 같이 클라이언트와의 연결 정보를 표시하며, 클라이언트로부터 IoC 데이터 등록 요청을 받아 블록체인 내에 저장/등록하는 과정을 수행한다.



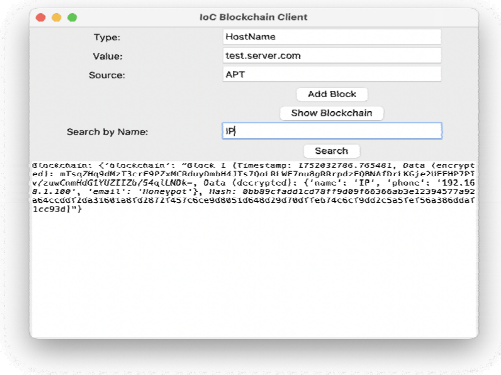
[Fig. 9] IoC Blockchain Server Module

블록체인 시스템에 대해 아래 그림 10과 같이 블록체인에 저장/등록된 정보에 대한 검색 과정을 수행할 수 있다. 클라이언트에서 IoC 정보에 대해 키워드 검색 과정을 수행하면 스마트 컨트랙트 정보를 토대로 서버 내 블록체인에 저장된 해당 블록 정보를 검색하고 이를 서버에 출력하는 기능을 구현하였다.



[Fig. 10] IoC Blockchain Data Request and Response

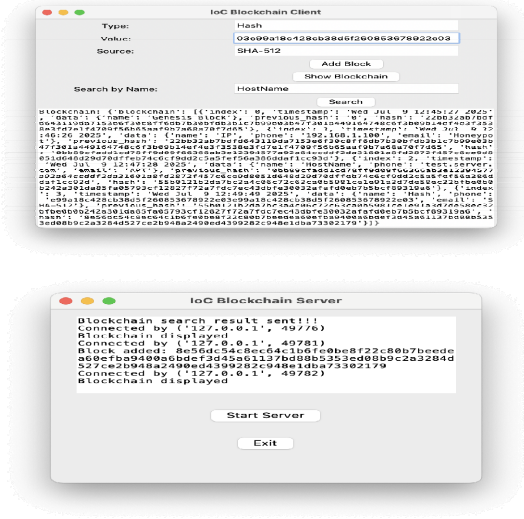
클라이언트에서는 아래 그림 11과 같이 IoC 데이터 Type 정보를 중심으로 검색어를 입력하면 서버에 저장된 IoC 블록체인에서 해당 블록을 검색하고 이를 클라이언트 윈도우에 표출하도록 구현하였다.



[Fig. 11] IoC Blockchain Search Result

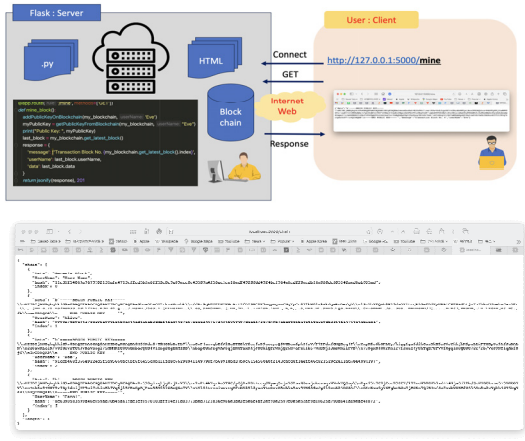
본 연구에서 구현한 IoC 블록체인 시스템은 Python 언어를 이용하여 개발하였으며 범용 블록체인 시스템으로 확장이 가능하며, PyCryptodome 암호화 모듈을 사용하여 블록체인 정보에 대한 암복호화 기능을 제공하며, 멀티 쓰레드 기반 TCP 연결 방식의 클라이언트/서버 방식으로 연동되므로 신뢰성을 제공하며, SHA-512 해시값을 토대로 블록체인 내에 저장된 IoC 데이터에 대한 위변조 방지 기능을 제공한다.

본 연구에서 구현한 시스템을 이용할 경우 아래 그림 12와 같이 사이버 공격 발생시 수집되는 IoC 정보에 대해 서버내 블록체인 정보로 저장하게 되며, 해당 정보를 손쉽게 공유할 수 있게 되며, 또한 각각의 클라이언트에서는 블록체인 내에 저장된 IoC 정보를 안전하게 추출할 수 있는 기능을 제공한다.



[Fig. 12] Client/Server based IoC Blockchain System

추가적으로 이용 과정의 편리성 및 사용자 인터페이스 기능을 향상시키기 위해서 아래 그림 13과 같이 Flask 기반 웹 인터페이스 방식으로도 동작할 수 있도록 추가 기능을 구현하였다.

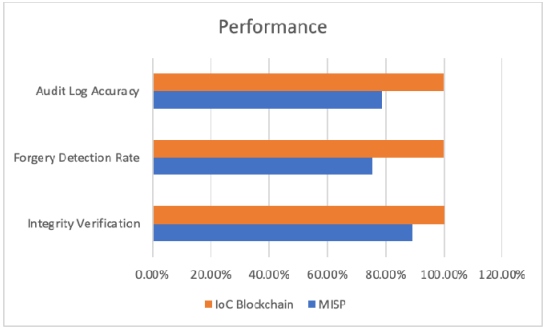


[Fig. 13] Flask based IoC Blockchain System

4.4 성능 비교 평가

사이버 공격에 대한 정보 공유 및 대응 과정에서의 효

율성을 중심으로 성능을 비교 평가하였다. 제안한 블록체인 기반 침해지표 공유 메커니즘의 성능을 평가하기 위하여, 기존 MISP[7] 기반 IoC 공유 시스템과의 비교 실험을 수행하였다. 성능 평가는 세 가지 항목을 중심으로 이루어졌으며, (1) 무결성 검증 성공률, (2) 정보 공유 지연 시간 및 (3) 위·변조 대응 능력 및 감사 추적 기능에 대해 성능을 비교 분석하였다. 성능 비교 평가를 위해 MISP 서버 1대, 클라이언트/서버 블록체인 노드 각 1개를 이용하였으며, 가상 내부망(LAN)에서 총 150건의 IoC 침해지표 항목(IP, 해시, 도메인, TTP 등 포함)을 대상으로 성능을 비교 분석하였다. 성능 비교 결과 아래 그림과 같이 제안한 IoC 블록체인 시스템은 기존의 MISP 시스템과 성능을 비교하였을 경우 블록체인 감사 추적 기능의 정확도가 21.1% 향상되었으며, 위변조 검출 성능을 24.3%, 그리고 무결성 검증 성능은 10.8% 각각 향상된 것으로 나타났다. 또한 IoC 데이터에 대한 공유 시간 지연은 기존 MISP 대비 0.9초 개선된 것으로 나타났다.



[Fig. 14] Performance Comparison

성능 비교 결과를 요약하면 다음과 같다. 첫째로 무결성 검증 측면에서는 블록체인의 해시 기반 검증 절차와 스마트 컨트랙트의 자동화된 검증 로직이 실효성 있게 작동되는 것을 확인할 수 있었다. 또한 기존 MISP 시스템은 공유된 IoC의 변경 여부를 외부에서 실시간으로 확인하기 어렵지만, 제안 시스템에서는 모든 트랜잭션 기록이 블록에 포함되어 완전한 감사 추적이 가능하였다. 지연 시간 측면에서는 블록체인의 블록 생성 주기(약 2초)가 일부 성능 제한 요소로 작용하였으나, 실제 공유 지연 시간은 평균적으로 오히려 감소하였다. 이는 데이터 전송 및 검증 절차가 중앙 서버를 거치지 않고 Peer 간 직접 이루어졌기 때문이다. 결국 제안한 시스템은 정보 공유의 신뢰성과 실시간성, 무결성 보장 측면에서 기존 IoC 공유 모델보다 우수한 성능을 보였으며, 특히 사이버 위협 대응 과정에서의 자동화 및 감사 기능 구현에 있어 실질적인 효과가 있음이 확인되었다. 본 연구에서는 블록체인 기반 IoC 공유 시 발생하는 처리 속도를 비교하였지만, 전체적인 트랜잭션 처리량과 네트워크 부하에 대해서는 정량적으로 비교할 수 없었고, 합의 알고리즘별 성능 비교 역시 제외하였다.

블록체인 기술 적용시 PyCryptodome 기반 암복호화 모듈을 적용하였으며, 해시값을 이용하여 데이터에 대한 무결성을 확인/검증하였으므로 블록체인 내에 저장된 데이터에 대한 위변조는 완벽하게 방지할 수 있다. 또한, RSA 공개키를 이용하여 블록체인 정보에 대한 저장 및 검증 과정을 수행하였으므로 참여자에 대한 권한 오남용을 방지할 수 있다. 다만, 본 연구에서 설계 및 구현한 내용은 실제 사이버 보안 환경(기업 보안 시스템 등)을 대상으로 추가적인 접목 및 테스트 과정이 필요하다.

5. 결론

본 연구에서는 사이버 공격 발생 시 생성되는 침해지표를 보다 효과적으로 공유하기 위해 블록체인 기술 기반의 IoC 정보 생성 및 공유 메커니즘을 제안하였다. 기존에 일반적으로 사용하였던 중앙 집중형 IoC 공유 시스템의 한계인 무결성 검증의 어려움, 단일 실패 지점(SPOF), 감사 추적 불가능성 등의 문제점을 개선하기 위해, 본 논문에서는 다이아몬드 모델 기반 IoC 형태로 구조화하였으며, 범용성 및 구현의 용이성을 제공하기 위해 PyCryptodome 기반 암호학적 모듈 사용, 스마트 컨트랙트를 활용한 블록체인 저장 및 API 연동에 이르는 통합 아키텍처를 설계 및 구현하였다.

제안된 시스템은 사이버 공격 발생시 해당 위협 정보를 IoC 정보로 실시간 생성하고, 이를 정규화하여 블록체인 노드 내에 등록함으로써 위변조 방지 기능을 제공하며, 다양한 내외부 CTI 기관 간의 상호 신뢰 기반 협업 및 공유 체계를 제공한다. 특히, 본 논문에서 제시한 Python 기반 경량 블록체인 구현 예제는 범용성과 확장성을 동시에 제공하며, 향후 Hyperledger Fabric 등과 같은 블록체인 보안 시스템에 적용 가능함을 입증하였다.

제안한 메커니즘 이용에 따른 성능 평가 결과, 제안한 시스템은 기존 MISP 기반 시스템 대비 무결성 검증 성공률과 감사 로그 추적 정확도에서 성능 향상을 보였으며, 정보 공유 지연 시간 측면에서도 효율적인 성능을 나타내었다. 또한 위협 정보에 대한 높은 위·변조 탐지율을

제공하여 사이버 공격 발생시 보안 신뢰성을 개선하였다. 이를 토대로 향후에는 AI 기반 자동 IoC 생성, 실시간 블록체인 등록 및 위협 시각화 기술 등에 적용 가능할 것으로 기대된다.

REFERENCES

[1] C. Miller and D. Ward, "Cyber Attack Response and the Role of Indicators of Compromise (IoC)," Journal of Cyber Defense and Security, Vol.18, No.1, pp.101-115, 2020.

[2] J. Zhao and A. Gupta, "A Comparative Analysis of IoC Formats for Cybersecurity," International Journal of Cyber Intelligence and Security, Vol.9, No.4, pp.313-327, 2019.

[3] D. Schmidt and M. Howard, "Real-Time Threat Intelligence and Automated IoC Sharing: An Industry Perspective," Journal of Cloud Computing and Security, Vol.24, No.3, pp. 102-118, 2020.

[4] M. Pawlowski and H. Schmidt, "Automated Threat Intelligence Collection and Indicator Transformation," Cybersecurity Technologies Review, Vol.16, No.2, pp.75-92, 2021.

[5] J. Stewart and S. Black, "Efficient Automated Indicator Transformation for Cyber Attack Detection," Journal of Cybersecurity Automation, Vol.5, No.1, pp.48-61, 2022.

[6] D. Reed and P. Cook, "A Study of Cyber Threat Intelligence Sharing Models," International Journal of Cybersecurity, Vol.11, No.2, pp.85-102, 2018.

[7] G. Caldarelli et al., "MISP: Malware Information Sharing Platform & Threat Sharing," in Proc. European Conf. on Cybersecurity, 2020.

[8] K. Scarfone and P. Mell, "Guide to Cyber Threat Information Sharing," NIST Special Publication 800-150, 2017.

[9] M. Blaise, "Threat Intelligence Sharing: The Role of MISP in the Modern Cybersecurity Landscape," Journal of Information Security, Vol.14, No.3, pp.245-261, 2019.

[10] D. Rothman, "TAXII™: Trusted Automated Exchange of Indicator Information," OASIS, 2017.

[11] R. Shilling and D. White, "STIX™: A Structured Threat Information Expression," OASIS, 2015.

[12] M. Chatziamanetoglou and K. Rantos, "Blockchain-Based Cyber Threat Intelligence Sharing Using Proof-of-Quality Consensus," J. Cybersecurity Privacy, Vol.3, No.1, pp.1-20, 2023.

[13] X. Gong and D. Lee, "BLOCIS: Blockchain-Based Cyber Threat Intelligence Sharing Framework," Electronics, Vol.9, No.3, p.521, 2020.

[14] A. Aneja et al., "A Survey on Cyber Threat Intelligence Sharing Based on Blockchain," J. Inf. Secur. Appl., Vol. 72, p.103383, 2023.

[15] H. Al-Dhaheri, M. Al-Kuwaiti, and K. Salah, "Leveraging Blockchain for Enhanced Threat Intelligence Sharing (CTIB)," Computer Security, Vol.135, p.103245, 2024.

[16] H. W, Lee, "Design and Implementation of an Indicators of Compromise Information Sharing Mechanism for Effective Cyber Attack Response," Journal of Internet of Things and Convergence, Vol.11, No.1, pp.93-100, 2024.

이 형 우(Hyung-Woo Lee) [종신회원]

■ 1994년 2월 : 고려대학교 컴퓨터학과 (학사)
■ 1996년 2월 : 고려대학교 컴퓨터학과 (석사)
■ 1999년 2월 : 고려대학교 컴퓨터학과 (박사)
■ 1999년 3월 ~ 2003년 2월 : 백석대학교 정보통신학부 교수
■ 2003년 3월 ~ 현재 : 한신대학교 AISW대학 교수

〈관심분야〉
사물인터넷, 정보보호, 모바일 보안 및 디지털 포렌식, 지능형 사이버공격 대응