

고속 신뢰 데이터 공유를 위한 DPU 오프로딩 기반 블록체인 앵커링 설계

박상준, 김종원*

광주과학기술원 AI융합학과

sjoonpark@gm.gist.ac.kr, *jongwon@gist.ac.kr

Design on DPU-offloaded Blockchain Anchoring for High-Speed Trusted Data Sharing

SangJoon Park, JongWon Kim*

Department of AI Convergence, Gwangju Institute of Science and Technology (GIST)

요약

객체 스토리지는 S3 인터페이스를 통해 대규모 비정형 데이터를 저장·공유하는 핵심 시스템으로 활용되고 있으며, 이에 따라 트랜잭션 수준의 감사 및 무결성 검증에 대한 요구가 증가하고 있다. 그러나 호스트 기반 트래픽 모니터링은 패킷 캡처, 메타데이터 파싱, 해시 계산 과정에서 상당한 연산 오버헤드를 유발하여 고성능 스토리지 환경의 성능 저하로 이어질 수 있다. 본 연구는 NVIDIA BlueField-2 DPU를 활용하여 S3 트래픽에 대한 감사 및 무결성 처리를 호스트로부터 오프로딩하는 블록체인 앵커링 아키텍처를 제안한다. 제안하는 시스템은 미러링된 네트워크 트래픽을 DPU 내부에서 처리하여 트랜잭션 메타데이터를 추출하고, 이를 머클 트리로 집계한 루트 해시만을 블록체인에 기록한다. 25GbE 환경에서 수행한 실험 결과, 제안하는 방식은 호스트 CPU 및 메모리 사용량을 Baseline 수준으로 유지하면서도 S3 트랜잭션 수준의 감사 데이터를 효과적으로 수집할 수 있음을 확인하였다.

I. 서론

객체 스토리지는 뛰어난 확장성과 HTTP 기반의 범용적인 접근성 덕분에, 대규모 비정형 데이터를 저장하고 공유하기 위한 핵심 인프라로 자리 잡았다. 최근 객체 스토리지는 단순 저장소를 넘어, AI 모델 학습과 데이터 분석을 위한 데이터 레이크 아키텍처의 핵심 구성 요소로 활용되고 있다.[1] 이와 같은 활용 범위의 확장으로 인해, 일부 개방적 또는 공유형 데이터 활용 환경에서는 데이터의 위변조 여부와 접근 이력을 검증할 수 있는 메커니즘이 중요하게 고려된다.[2]

데이터 공유 과정의 투명성을 확보하기 위해 감사 로그(Audit Log)를 블록체인에 기록하는 접근이 제안되어 왔으나, 이와 같은 보안·감사 처리가 고성능 스토리지 환경의 주 데이터 경로에서 수행될 경우 추가적인 처리 부하로 작용할 수 있다.[3] 스토리지 서버는 고속으로 유입되는 입출력(I/O) 요청을 처리하는 동시에 패킷 분석 및 암호화 해시 계산과 같은 부가 작업을 수행해야 하며, 이로 인해 처리량 요구가 증가할수록 연산 자원 소모가 지속적으로 발생한다. 결과적으로 이러한 오버헤드는 스토리지 서비스의 QoS에 영향을 미칠 수 있다.[4]

본 연구는 이러한 성능과 보안 간의 상충 관계를 완화하기 위해, NVIDIA BlueField-2 DPU를 활용한 DPU-offloaded Blockchain Anchoring 아키텍처를 제안한다. 제안하는 시스템은 호스트 CPU의 데이터 경로(Data Path) 처리 부담을 최소화하면서, 네트워크 인터페이스 단에서 트랜잭션 메타데이터를 즉시 추출하고 이를 머클 트리(Merkle Tree)로 집계하여 루트 해시만을 블록체인에 기록한다. 이를 통해 암호학적 무결성 검증과 감사 기능을 호스트 데이터 경로로부터 분리된 DPU 상에서 수행함으로써, 스토리지 서버의 I/O 성능 저하를 최소화하면서도 확장 가능한 보안·감사 체계를 구현한다.

II. 제안 아키텍처

본 연구에서 제안하는 시스템은 미러링된 네트워크 트래픽을 입력으로 받아 블록체인 앵커링 데이터로 변환하는 전 과정을 DPU 내부에서 파이프라인 형태로 처리한다. 그림 1과 같이, 해당 파이프라인은 DPU에 내장된 ARM 코어에서 동작하며, 필요에 따라 하드웨어 가속 기능을 활용함으로써 호스트 데이터 경로의 개입을 최소화하도록 설계되었다. 전체 아키텍처는 데이터 처리 흐름에 따라 (1) 재조립 및 메타데이터 추출, (2) 리프

해시 생성, (3) 배치 처리 및 머클 집계, (4) 이원화 전송의 네 단계로 구성된다.

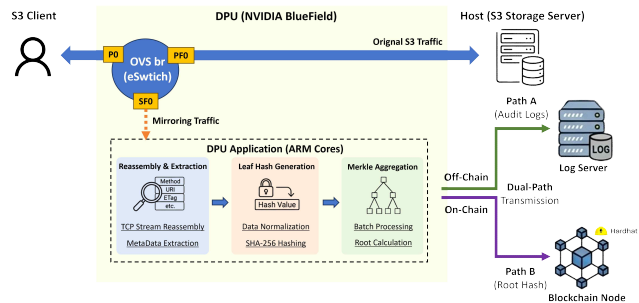


그림 1 DPU 오프로딩 기반 블록체인 앵커링 파이프라인 개요

1) TCP 재조립 및 메타데이터 추출 (Reassembly & Extraction): 고속 네트워크에서 파편화되어 유입되는 패킷들을 DPU 내에서 연속적인 TCP 스트림으로 복원(Reassembly)한다. 이후 경량화된 파서가 트랜잭션의 헤더 영역만을 분석하여 Method, URI, ETag 등 핵심 메타데이터를 추출하며, 트랜잭션 본문(Body) 데이터는 처리 대상에서 제외함으로써 처리 지연을 최소화한다.

2) 리프 해시 생성 (Leaf Hash Generation): 추출된 메타데이터는 필드 순서 통일 등 정규화(Normalization) 과정을 거쳐 표준 포맷으로 변환된다. 변환된 데이터는 SHA-256 알고리즘을 통해 32바이트 길이의 고유한 리프 해시(Leaf Hash)로 생성되며, 이는 개별 트랜잭션의 무결성 검증을 위한 식별자로 사용된다.

3) 배치 처리 및 머클 집계 (Batch Processing & Merkle Aggregation): 블록체인의 처리 용량 한계를 극복하기 위해, 생성된 리프 해시들을 일정 단위(예: 1초 또는 1,000개)의 배치(Batch)로 묶어 머클 트리(Merkle Tree)를 구성한다. 이 트리의 최상위 노드인 루트 해시(Root Hash)는 해당 배치에 포함된 모든 트랜잭션의 무결성을 대변하는 단일한 증거값이 된다.

4) 이원화 전송 (Dual-Path Transmission): 최종 데이터는 목적에 따

라 분리 전송된다. 상세 감사 내역이 담긴 {Leaf Hash, Metadata}는 로그 서버(Audit Log)로 전송되어 검색 편의성을 제공하고(Off-Chain), 위변조 검증을 위한 {Root Hash}는 블록체인 네트워크(Anchor)로 전송되어 데이터의 불변성을 보장한다(On-Chain).

III. 실험 및 평가

3.1 실험 환경

실험은 AMD EPYC 7513 32코어 프로세서(64 스레드), 128GB 메모리를 탑재한 호스트 노드와 NVIDIA BlueField-2 DPU(ConnectX-6)를 25GbE 네트워크로 연결한 환경에서 수행되었다. 단일 노드에 MinIO 서버를 구성하고 Warp 클라이언트로 트래픽을 생성하여 모니터링 오버헤드를 측정하였다.

3.2 실험 시나리오

실제 S3 서비스 운영 패턴을 반영하기 위해 Warp 벤치마크 도구를 활용한 2단계 워크로드를 설계하였다. 1단계는 초기 데이터 적재를 모사한 위밍업(5분, PUT 중심), 2단계는 일반적인 운영 상황을 재현한 혼합 워크로드(10분, GET 80% / PUT 15% / DELETE 5%)로 구성하였다. 이는 클라우드 스토리지의 전형적인 사용 패턴인 초기 대량 업로드 후 읽기 중심 운영을 반영한다. 본 실험은 HTTP/1.1 평문 트래픽을 대상으로 하며, TLS 암호화 환경 및 HTTP/2는 고려하지 않았다.

3.3 비교 대상

감사 처리 위치에 따른 성능 영향을 정량화하기 위해 세 가지 구성을 비교하였다.

- **Baseline:** 감사 처리 없이 순수 워크로드만 실행
- **Host Processing:** 감사 처리를 호스트 CPU에서 수행
- **DPU Offloading:** 제안하는 방식으로 감사 처리를 DPU로 오프로딩

Host Processing 구성에서는 호스트 CPU에서 S3 트래픽을 캡처한 뒤, HTTP 요청 메소드, URI, 응답 코드 등의 L7 메타데이터를 파싱하고 SHA-256 해시 계산을 수행하도록 구성하였다. 이는 제안하는 DPU 오프로딩 파이프라인과 동일한 처리 단계를 호스트 상에서 모사하기 위함이다. 각 구성에 대해 CPU 사용률, 메모리 사용량, 네트워크 처리량을 측정하였으며, 모든 실험은 동일 조건에서 5회 반복 수행 후 평균값을 사용하였다.

3.4 실험 결과

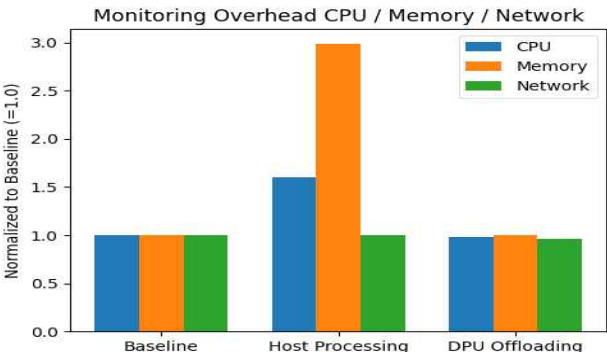


그림 2 구성 별 호스트 자원 사용률

Host Processing 구성에서는 트래픽 캡처, L7 메타데이터 파싱, 해시 계산으로 인해 CPU 사용률이 baseline 대비 약 55% 증가하고, 메모리 사용량이 최대 3배 이상 증가하였다. 네트워크 처리량 또한 사용자 공간 패킷 처리 오버헤드로 인해 전반적인 감소 경향을 보였다. 반면, DPU Offloading 구성에서는 호스트 CPU 및 메모리 사용량이 baseline 수준을

유지하여, 제안하는 방식이 호스트 자원 소모 없이 감사 처리를 수행함을 확인할 수 있었다. 네트워크 처리량은 약 4~6% 감소하였으나, 이는 DPU 내부 처리로 인한 제한적인 지연이 벤치마크 환경에서 반영된 결과로 분석된다.

종합적으로, DPU Offloading 방식은 호스트 자원 사용을 최소화하면서 L7 감사 및 무결성 처리를 지원하는 효율적인 접근임을 실험적으로 입증하였다

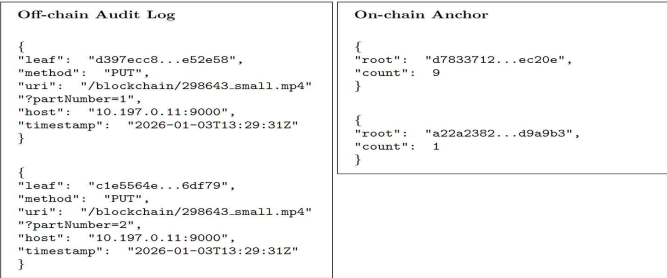


그림 3 오프체인 감사 로그와 온체인 머클 루트 앵커 예시

그림 3은 제안한 시스템을 통해 실제 S3 트랜잭션으로부터 생성된 감사 로그와 블록체인 앵커링 결과의 예시를 보여준다. 왼쪽은 오프체인 로그 서버에 저장된 트랜잭션 메타데이터와 대응되는 리프 해시를 나타내며, 오른쪽은 동일 배치에 대해 생성되어 블록체인에 기록된 머클 트리 루트 해시를 보여준다. 개별 트랜잭션의 무결성은 해당 리프 해시와 머클 증명을 통해 온체인 루트 해시와의 일치 여부로 검증할 수 있다.

IV. 결론

본 연구는 BlueField-2 DPU를 활용하여 S3 트래픽에 대한 감사 및 무결성 처리를 호스트로부터 오프로딩하는 아키텍처를 제안하고 구현하였다. 제안하는 방식은 네트워크 계층에서 독립적으로 동작함으로써 호스트 성능에 영향을 주지 않으면서도 트랜잭션 수준의 가시성을 제공할 수 있음을 통해 확인하였다.

현재 구현은 단일 노드 및 HTTP/1.1 평문 트래픽 환경을 대상으로 검증되었으며, 향후 TLS 암호화 및 다중 노드 환경으로의 확장이 요구된다. 그럼에도 불구하고, 본 연구는 DPU 기반 오프로딩이 고성능 스토리지 환경에서 확장 가능한 감사 체계를 구현하는 실질적인 대안이 될 수 있음을 보여준다.

ACKNOWLEDGMENT

본 연구는 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-대학 ICT연구센터(ITRC)의 지원(IITP-2026-RS-2021-II211835)과 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No. 2019-0-01842, 인공지능대학원지원(광주과학기술원)).

참 고 문 헌(수정)

[1] P. Jain et al., "Analyzing and Comparing Lakehouse Storage Systems," in Proc. Conf. Innov. Data Syst. Res. (CIDR), 2023.

[2] W. Ma, X. Wei, and L. Wang, "A security-oriented data-sharing scheme based on blockchain," Appl. Sci., vol. 14, no. 16, p. 6940, 2024.

[3] M. H. Rakib et al., "A blockchain-enabled scalable network log management system," J. Comput. Sci., vol. 18, no. 6, pp. 496-508, 2022.

[4] P. Hamandawana, D.-J. Cho, and T.-S. Chung, "Speed-Dedup: A new deduplication framework for enhanced performance and reduced overhead in scale-out storage," Electronics, vol. 13, no. 22, p. 4393, 2024.