Journal of KIIT. Vol. 24, No. 6, pp. 217-227, Jun. 30, 2026. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2026.24.6.217

정책 준수 검증을 위한 영지식증명 기반 텔레메트리 데이터 무결성 메커니즘 제안

김진수*, 최은선**, 박남제***

A Zero-Knowledge Proof-based Telemetry Data Integrity Mechanism for Policy Compliance Verification

Jinsu Kim*, Eunsun Choi**, and Namje Park***

이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(RS-2026-25498234)

요 약

텔레메트리 데이터의 무결성은 자동화와 안전 의사결정의 핵심 기반이지만, 기존 방식은 애플리케이션 신뢰와 원시데이터 보관에 의존하여 프라이버시 보호와 감사 가능성 측면에서 한계를 가진다. 이에 본 논문은 값을 공개하지 않고 정책 준수 여부를 입증할 수 있는 영지식증명 기반의 무결성 메커니즘을 제안한다. 제안된 메커니즘은 커밋, 증명, 온체인 검증, 정책 버전 앵커링, 집계 운용을 단일 절차로 통합하여, 데이터 노출 없이 정책 준수 판정과 재현 가능한 감사를 가능하게 한다. 또한 블록체인에 판정 결과와 정책 버전을 기록하여 판정의 불변성과 재현성을 확보하고, 집계 증명을 통해 다건 제출의 검증 호출을 줄여 검증 효율성을 향상시킨다. 결과적으로 본 논문은 데이터 무결성, 프라이버시, 감사 가능성, 비용 효율성을 동시에 충족하는 새로운 텔레메트리 신뢰 모델을 제시한다.

Abstract

Ensuring the integrity of telemetry data is essential for automation and safety-critical decision making. However, existing methods rely on application-level trust and centralized raw data storage, limiting privacy protection and auditability. This paper proposes a Zero-Knowledge Proof based integrity mechanism that verifies policy compliance without disclosing data values. By integrating commitment, proof generation, on-chain verification, and policy version anchoring, the proposed model enables reproducible and privacy-preserving auditing. Anchoring policy updates and results on blockchain ensures immutability and reproducibility, while batch verification reduces verification overhead, thereby unifying data integrity, privacy, and auditability.

Keywords
telemetry, integrity, zero-knowledge proof, on-chain verification, aggregated proofs

* 제주대학교 사이버보안인재교육원 연구원
- ORCID: https://orcid.org/0000-0003-1009-3928
** 광주교육대학교 컴퓨터교육학과 교수
- ORCID: https://orcid.org/0000-0001-6384-5324
*** 제주대학교 초등컴퓨터교육전공, 융합정보보안학과 교수(교신저자)
- ORCID: https://orcid.org/0000-0003-4434-8933

· Received: Sep. 29, 2025, Revised: Jun. 10, 2026, Accepted: Jun. 13, 2026
· Corresponding Author: Namje Park
Dept. of Computer Education, Teachers College, Jeju National University, 61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 63294, Korea
Tel.: +82-64-754-4914, Email: namjepark@jejunu.ac.kr

Ⅰ. 서 론

현대의 설비와 환경 센서가 생성하는 텔레메트리는 자동화와 안전, 규정 준수 판단을 떠받치는 핵심 데이터다. 그럼에도 현장의 무결성 보장은 애플리케이션 신뢰와 원시데이터 보관에 기댄 사례가 많아, 값 노출 위험과 과도한 보관 부담, 분산된 로그로 인한 감사 비용을 키운다[1]. 대규모 장치가 고빈도로 제출하는 환경에서는 확장성과 지연, 비용을 동시에 관리해야 하며, 정책이나 보정 값이 바뀌어도 과거 판정을 동일 조건으로 재현할 수 있어야 한다. 이러한 요구를 만족하는 구조적 대안이 필요하다[2][3].

하지만, 원시값 중심 검증은 데이터 최소 공개 원칙과 충돌하고, 접근 권한 관리에 따른 법적 책임을 증폭시킨다. 판정 근거가 애플리케이션과 데이터베이스에 분산되면 변경 가능성이 남고, 정책과 보정의 변동이 있을 때 과거 판정의 재현성이 흔들린다. 장치의 폐기·위변조 여부를 즉시 확인하기 어렵고, 중복 제출과 재전송은 검증 자원을 불필요하게 소모한다. 이처럼 무결성 보장은 데이터 노출, 기록의 가변성, 버전 관리의 취약성 등 복합 병목에 갇혀 있다[4][5].

이에 따라, 영지식증명은 값 공개에 의존하는 기존 검증의 한계를 줄이는 실질적 해법이 된다. 장치 단계에서 값·난수·메타데이터를 결속한 커밋을 만들고, 공개된 정책 제약을 만족한다는 사실만을 증명함으로써 값 자체를 노출하지 않고도 신뢰 가능한 판정에 도달한다[6]. 판정과 정책 버전을 블록체인에 고정하면 기록의 변경 가능성이 사라지고 감사와 재현성이 확보된다. 또한 장치 등록과 커밋 중복 차단을 사전 단계로 두어 위변조·재전송을 억제하고, 다건 제출은 집계 증명으로 묶어 검증 호출을 줄여 비용과 지연을 낮춘다. 공개 입력을 최소화하는 설계는 링크 가능성을 줄여 프라이버시를 보전한다[7][8].

따라서, 본 논문은 위 대안을 구체화하여, 텔레메트리 제출에서 판정 기록까지를 하나의 메커니즘으로 정의하고 프로토콜 수준의 명세와 간결한 정식화를 제시한다. 커밋과 증명, 온체인 검증과 불변 기록, 정책 버전 앵커링, 집계 운용을 단일 절차로 통합함으로써 값 비공개 상태에서 정책 준수 판정과 재현 가능한 감사를 가능하게 한다.

Ⅱ. 관련 연구 분석

2.1 텔레메트리 무결성 기법 분석

분산 환경에서의 무결성 보장은 오랫동안 전송 보호, 디지털 서명·해시, 보안 감사 로그, 신뢰실행환경(TEE, Trusted Execution Environment)의 원격증명에 의해 달성되어 왔다. 이 계열은 "무슨 일이 발생했는가"를 변경 불가능한 형태로 남기고, 사후 재현과 책임 추적을 가능하게 만든다. 그러나 값 공개를 최소화한 상태에서 정책 준수의 의미론적 검증을 제공하는지는 별도의 문제로 남아 있다[9].

보안 감사 로그는 로그 항목을 암호학적으로 연쇄 결속하여 삭제·삽입·수정을 탐지하는 tamper-evident 구조를 제공하며, 침해 이후에도 포렌식 가능한 기록을 유지한다. 분산 계정성 프레임워크는 서명 로그와 기준 구현에 대한 재실행 대조를 결합하여, 관측 가능한 비정상 행위를 특정 주체에 귀속시키는 실용적 책임성을 달성한다. 한편 TEE 기반 원격증명은 하드웨어 신뢰 뿌리를 이용해 플랫폼·코드 상태를 제3자에게 증명하는 운용 모델을 제공하며, 데이터센터 환경에서 제3자 검증 인프라를 갖춘 형태로 정교화되어 왔다[10][11]. 더 나아가 이 세 범주는 데이터의 이동·저장·실행이라는 서로 다른 위협 면을 분담함으로써 동일 사건에 대한 증거를 상호 보완적으로 남기며, 로그는 발생 사실과 순서를, 계정성은 행위의 정당성을, 원격증명은 실행 환경의 신뢰성을 계층적으로 뒷받침한다.

2.2 블록체인 앵커링 분석

블록체인 앵커링은 해시와 같은 데이터 요약을 불변 장부에 고정하여, 제3자가 독립적으로 변경 여부를 검증할 수 있게 하는 방법이다. IoT 맥락에서는 대량의 센서 스트림에 대해 출처와 변환 경로를 남기고, 사건 시점·책임 추적을 지원하는 감사 인프라로 활용이 확산되고 있다. 앵커링된 요약은 블록

타임스탬프와 높이와 결합되어 사건의 시간적 순서를 고정하며, 감사자는 원본에 접근하지 않고도 요약 대조만으로 위·변조 여부를 판단할 수 있다[12].

운용 패턴은 대체로 오프체인 저장과 온체인 요약으로 구성된다. 장치/엣지에서 원본을 저장소에 적재하고, 계약에는 콘텐츠 무결성을 식별하는 커밋 해시, 수집 시각·장치 식별자·처리 단계 등 최소 메타데이터, 버전·스키마 식별자를 기록한다. 단건 앵커링의 비용을 줄이기 위해 머클 배치나 롤업형 집계가 쓰이며, 체인 이벤트를 인덱싱해 역질의와 기간별 감사 보고를 구성한다. 권한형 컨소시엄 체인에서는 스마트컨트랙트 기반 감사 로그와 장치/운영자 등록, 중복 커밋 차단, 정책·스키마 버전 필드 등을 통해 추적성과 형상 관리를 동시에 달성한다. 공용 체인을 이용하는 경우에는 L2·배치 주기·가스 상한으로 비용/지연을 조절하고, 체인 재구성 대비 최소 확정성 깊이를 정해 운영한다[13][14].

따라서 앵커링은 불변 이력과 제3자 검증을 강화하는 선택적 구성으로 유효하지만, 정책 준수의 의미론적 판정은 별도의 체계가 필요하며, 본 논문의 제안은 이 부분을 영지식증명 기반 메커니즘으로 해결한다.

2.3 관련 연구 분석

현행 접근을 종합하면 두 축의 공백이 뚜렷하다. 값은 숨긴 채로 정책 준수 여부를 즉시 판단하는 형식적 검증 수단이 부족하고, 불변 장부에 남는 기록이 판정의 의미론과 충분히 결합되지 않아 동일 조건으로 맥락을 복원하기 어렵다. 대량 제출에서의 비용과 지연, 공개 입력이 남기는 링크 가능성, 정책이나 보정값의 변경이 과거 판정의 재현성을 흔드는 문제도 동시에 나타난다[15]. 이러한 한계는 값 비공개 상태에서 정책 제약 충족을 증거로 제시하고, 판정과 정책 버전을 일관되게 고정하며, 집계로 검증 호출을 억제하는 설계가 필요함을 시사한다.

B. Benedikt et al.의 연구[16]에서는 신뢰 설정 없이도 짧은 범위증명과 다중 범위의 집계 검증을 제시하여, 값 비공개 상태에서 범위·형식 제약을 실용적으로 판정할 수 있음을 보였다. J. Groth의 연구[17]에서는 상수 크기 증명과 빠른 검증을 갖춘 SNARK를 제시해 온·오프체인 어디서든 정책 회로 검증의 단가를 크게 낮출 수 있음을 입증했다. M. Mary et al.의 연구[18]에서는 보편·업데이트 가능한 SRS를 지원해 정책·회로 변경이 잦은 환경에서 설정 재사용을 가능케 하고, 배치 검증 조력자 모델로 대량 검증의 한계를 완화했다. Chiesa et al.의 연구[19]에서는 보편·업데이트 가능한 SRS를 유지한 전처리형 zkSNARK로, 검증키/정책 버전 관리 부담을 줄이면서도 빠른 검증을 달성하는 방법을 제시했다. Narula et al.의 연구[20]에서는 원장 데이터 노출 없이도 합계·제약 충족 여부를 감사자가 질의·검증할 수 있는 프로토콜을 구현해, 값 비공개 정책 검증의 감사 가능성을 실제 시스템 수준에서 증명했다.

선행 연구에서는 비공개 제약 검증, 짧은 증명·빠른 검증, 보편/업데이트 가능한 설정, 집계·재귀 검증, 비공개 감사 등 개별 능력을 확장해 왔으나, 텔레메트리 파이프라인을 아우르는 엔드투엔드 운용 모델은 부족하다[21]-[22]. 본 논문는 최소 공개 입력의 커밋 - 증명 흐름을 중심으로 장치 등록, 커밋 중복 차단, 정책 버전·검증키·판정의 결속, 단건/집계 제출, 이의 절차를 하나의 상태기계로 통합한다. 판정과 정책 버전은 투명 로그 또는 불변 원장에 선택적으로 고정해 재현 가능성을 확보하고, 집계·재귀 운용으로 비용과 지연을 억제한다. 결과적으로 값 비공개, 정책 준수의 형식적 판정, 감사 가능성, 확장성을 동시에 충족하는 실무 지향 메커니즘을 제시한다.

III. 영지식증명 기반 텔레메트리 무결성 메커니즘 제안

본 장에서는 텔레메트리 전 과정을 값 비공개 상태로 검증하고 결과를 변경 불가능한 원장에 고정해 무결성을 높이는 메커니즘을 제안한다. 측정 시점에 장치는 값과 난수와 최소 메타데이터를 결속한 커밋을 만들고 공개 정책 제약을 만족한다는 증명을 함께 생성한다. 제출 자료는 블록체인에서 정책 버전에 따른 기준으로 검증되며 수락 여부와 버전이 블록 시간과 함께 기록된다. 집계 증명을 적용하면 여러 제출을 하나로 압축해 비용과 지연을 줄이되 결속성과 정당성과 영지성과 불변 기록이라는

핵심 보장은 유지된다. 또한 공개 입력은 정책 버전·장치 식별자·시간창 등 최소 필드로 제한해 링크 가능성을 낮춘다.

3.1 약어 정리

본 절은 그림과 표에서 쓰이는 핵심 약어를 문장으로 정의한다.

표 1은 본 논문에서 사용하는 약어를 정의한 것이다. y는 검증에 필요한 최소 공개 필드 묶음으로, 보통 정책 버전·장치 식별자·허용 시간창·보정 해시·커밋 해시가 포함된다. w는 외부에 공개하지 않을 비공개 입력 묶음을 의미한다.

표 1. 기호/약어 정리
Table 1. Notation and abbreviations

Abbrev.	Definition
y	Minimal set of public fields required for verification.
w	Private inputs kept off-chain.
R(y, w)	Policy constraints that must hold simultaneously.
VK	Verification key for the specific circuit/policy version used during proof checking.
Y_AGG	Aggregated public inputs that normalize/pack multiple yiy_iinto a single verification instance.
P_AGG	Aggregated proof that compresses multiple pip_iinto a single verifiable proof.
C_LIST	Ordered list of commit hashes included in a batched submission.
TX	On-chain submission unit.
tx_hash	Transaction hash used for acknowledgment and traceability.
H(·)	Hash/commit function that binds value, nonce, and metadata to produce the commitment.

R(y, w)는 값이 따라야 하는 정책 제약의 논리 묶음이며, 범위/형식 적합성, 변화율 기반 일관성, 제출 지연 한도에 의한 신선도, 보정 데이터와의 일치, 커밋과의 결속으로 구성된다. VK는 특정 정책·회로 버전에 대응하는 공개 검증 파라미터다.

집계 처리를 위해 Y_AGG는 복수의 공개 입력을 하나로 정규화·압축한 표현이며 P_AGG는 복수의 증명을 단일 검증이 가능하도록 묶은 결과다. C_LIST는 배치 제출에 포함되는 커밋 해시 목록으로 사후 감사 시 집계 단위와 개별 제출을 연결한다.

TX는 온체인 제출의 단위이고, tx_hash는 제출 접수 확인과 추적을 위한 식별자다. 마지막으로 H(·)는 값·난수·메타데이터를 결속해 커밋을 생성하는 해시/커밋 함수를 의미한다.

3.2 구성 요소 정리

제안 메커니즘은 종단 장치, 엣지 수집자, 서버, 블록체인의 네 가지 구성요소로 구성되며, 블록체인은 다섯 개의 기능적 요소로 정의한다.

표 2는 제안 메커니즘의 구성 요소를 보이는 것이다. 종단 장치(Device)는 센서 값을 취득하고, 값과 메타데이터를 결속한 커밋과 정책 준수 여부를 입증하는 증명을 생성해 한 번의 트랜잭션으로 제출한다. 엣지 수집자(Edge aggregator)는 여러 장치에서 들어온 제출을 수집해 형식과 타임스탬프를 정규화하고, 중복을 제거한 뒤 집계 증명으로 압축해 블록체인에 전달함으로써 비용과 지연을 줄인다. 서버(Server)는 블록체인에서 발생하는 판정 결과와 정책 버전, 블록 정보를 구독하여 상태를 시각화하고 경보·리포트를 제공하되, 검증의 신뢰 근원으로 사용되지는 않는다. 블록체인(Blockchain)은 정책과 장치 상태를 점검한 후 영지식 검증을 수행하고, 판정과 정책 버전을 불변 기록하며 필요 시 이의 제기를 처리한다.

표 2. 제안 메커니즘 구성 요소
Table 2. Proposed mechanism components

Component	Primary role
Device	Measure data, create commitment, create zero-knowledge proof, submit a single transaction
Edge aggregator	Collect submissions from multiple devices, normalize them, submit an aggregated transaction
Server	Subscribe to blockchain events, monitor status, trigger alerts and reporting
Blockchain	Check policy and device status, verify proofs, record verdicts immutably, handle disputes

표 3은 블록체인의 기능적 구성 요소를 보이는 것이다. PolicyRegistry는 정책·회로 버전을 관리하고 검증 기준을 제공하며, DeviceRegistry는 장치의 등록과 상태, 키 수명주기를 통제한다. 두 레지스트리는 블록체인에 의해 불변성이 보장되지만, 실제 등록 및 검증 트랜잭션은 Fog Operator가 수행한다. 이에 따라 운영 주체의 무결성과 키 관리가 시스템 신뢰의 전제 조건으로 가정된다. ZKVerifier는 제출된 공개 정보와 증명을 바탕으로 영지식 검증을 수행해 수락 또는 거절을 결정한다. CommitStore는 판정과 정책 버전, 블록 정보를 변하지 않게 기록하고 중복 제출을 차단하며, 외부로 이벤트를 발행한다.

Dispute는 이의 제기와 보완증빙을 받아 재검증을 트리거하고, 갱신된 판정을 기록해 감사 가능성을 높인다.

표 3. 블록체인 기능적 구성 요소
Table. 3. Blockchain functional components

Component	Primary role
PolicyRegistry	Versions policies/circuits and provides the verification key or circuit hash
DeviceRegistry	Manages device enrollment and status (valid/revoked) and handles key rotation
ZKVerifier	Executes zero-knowledge proof verification and produces accept/reject decisions
CommitStore	Permanently records commit hash, policy version, verdict, and block; emits events; prevents duplicate submissions
Dispute	Receives appeals and evidence hashes, triggers re-verification, and records updated verdicts

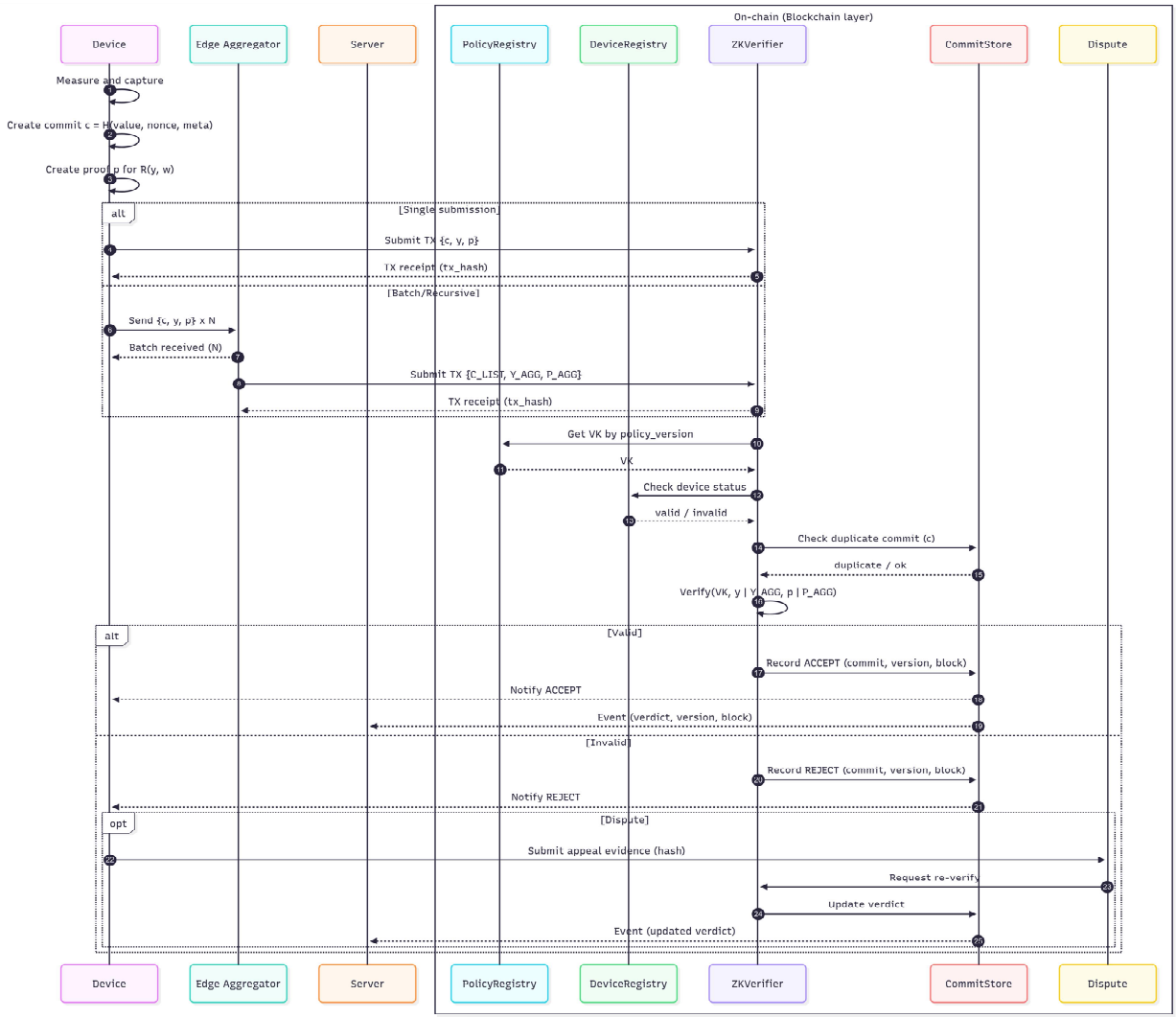


그림 1. 제안 메커니즘 구성요소별 데이터 흐름 설계도
Fig. 1. Data flow diagram of the proposed Mechanism

3.3 증거 생성과 온체인 검증 절차

제안 메커니즘에서는 측정 시점부터 블록체인 기록까지의 전 과정을 하나의 프로토콜로 묶어, 값을 드러내지 않고도 정책 준수 여부를 기계적으로 확인하고 그 결과를 변경 불가능하게 고정하는 방법을 제시한다.

그림 1는 제안 메커니즘의 구성요소와 블록체인의 기능적 구성요소간 데이터 처리 및 전파 흐름을 보이는 것이다.

측정이 발생하면 장치는 값(v)과 난수(r)와 메타데이터(m)를 해시 함수에 결속해 커밋(c)을 만든다. 이때 커밋 함수(H)를 사용하며 관계는 식 (1)과 같이 표현된다.

$$c = H(v, r, m) \tag{1}$$

장치는 이어서 공개 입력(y)와 비공개 입력(w)를 준비하고, 공개된 정책 제약 $R(y,w)$를 만족한다는 증명(p)를 생성한다. 공개 입력에는 정책 버전과 장치 식별자, 허용 시간창과 보정 데이터의 해시, 그리고 커밋 해시가 포함되며 값 자체는 공개되지 않는다. 신선도는 시간창(Time window)을 기준으로 하여 측정 시각이 식 (2)와 같이 범위 내에 있는지를 통해 판정한다.

$$t_{\min} \le t_{meas} \le t_{\max} \tag{2}$$

제출은 두 가지 경로로 진행된다. 단건 제출의 경우 장치는 커밋과 공개 입력, 증명을 하나의 트랜잭션으로 전송하고 영수증 역할의 tx_hash를 수신한다. 다수 측정이 모인 상황에서는 엣지 수집자가 여러 장치의 제출을 모아 형식과 시각을 정규화하고 중복을 제거한 다음, 커밋 목록(CLIST)와 집계 공개 입력(YAGG), 집계 증명(PAGG)로 압축하여 단일 트랜잭션으로 보낸다. 이 단계에서 엣지는 원시값을 해석하지 않고 이미 봉인된 항목만 재포장하므로 프라이버시와 결속성이 유지된다.

온체인에 도달한 자료는 먼저 사전 점검을 거친다. 검증 모듈은 정책 레지스트리에서 해당 정책 버전의 검증키(VK)를 가져오고, 장치 레지스트리에서 제출 주체의 상태를 확인한다. 이어 기 접수된 커밋 해시의 원장(*CommitStore*)에서 동일 커밋 존재 여부(*Unique(c)*)를 조회해 재전송·중복을 차단한다. 이 중복 배제 조건은 식 (3)과 같이 형식화한다.

$$Unique(c) = c \in CommitStore \tag{3}$$

사전 점검이 통과되면 검증기는 공개된 정책 제약을 영지식 방식으로 판정한다. 단건 제출은 검증키(VK), 공개 입력(y), 증명(p)을 받아 해당 제출이 제약을 만족하는지 평가하고, 집계 제출은 집계 공개 입력(YAGG)집계 증명(PAGG)으로 묶인 여러 항목을 한 번에 평가하되 모든 항목이 참일 때에만수락한다.

수락(*ACCEPT*)으로 판정되면 검증기는 해당 제출의 결과를 커밋 저장소(*CommitStore*)에 한 행(Tuple)로 영구 기록하고, 동시에 서버가 구독할 수 있는 이벤트를 발생시킨다. 식 (4)는 기록되는 구조의 예시를 보이는 것이다.

$$(c, policy_{version}, verdict = ACCEPT, block) \in CommitStore \tag{4}$$

거절일 경우에도 사유와 함께 남겨져 사후 감사가 가능하며 필요하면 이의 절차로 보완 증빙의 해시를 제출해 재검증을 요청하고, 판정이 변경되면 갱신 기록과 이벤트가 추가된다. 이와 같은 연쇄적 흐름은 커밋을 통한 사후 변경 차단, 공개 입력 최소화에 따른 프라이버시 보전, 정책 제약에 근거한 기계적 판정, 온체인 앵커링에 의한 감사 가능성을 하나의 경로로 통합하여 텔레메트리 데이터의 무결성을 체계적으로 강화한다. Dispute 절차는 동일한 정책 기준 하에서 수행되며 이를 통해 재검증 과정에서 판정 기준의 일관성을 유지한다. 또한 블록체인의 불변성 특성에 따라 기존 판정 기록은 삭제되거나 변경되지 않으며, 재검증 결과는 새로운 기록으로 추가되어 판정 이력을 유지한다.

Ⅳ. 제안 메커니즘 구현 타당성 평가

4.1 실험 환경 구성

본 논문은 제안된 영지식 증명 기반 텔레메트리 데이터 무결성 검증 메커니즘의 동작 특성과 효율성을 검증하기 위해, macOS 로컬 환경에서 모듈 테스트를 위한 Python 기반 프로토타입을 구현하였다. 환경은 Python 3.9 기반으로 설정되었으며, 온체인 실험은 Ganache 로컬 블록체인을 통해 수행하였다. Ganache는 개발 및 테스트 환경을 위한 로컬 블록체인으로, 본 논문에서는 별도의 블록 확정 깊이를 설정하지 않고 트랜잭션이 블록에 포함되는 시점을 기준으로 기록을 처리하였다. 실험은 크게 오프체인 연산 성능 측정과 온체인 트랜잭션 비용 분석으로 구성되었다.

오프체인 실험에서는 텔레메트리 데이터의 입력 길이를 회로 복잡도의 척도로 설정하고, 각 구간에서 30회 반복 실험을 수행하여 증명 생성 및 검증 단계의 평균 처리시간을 산출하였다. 이를 통해 제안된 구조가 데이터 크기 증가에도 안정적인 검증 성능을 유지하는지를 관찰하였다. 온체인 실험에서는 단건 및 집계 단위의 정책 등록 트랜잭션을 실행하여 평균 가스비를 측정하고, 집계 크기별 누적 비용과 효율비를 계산하였다. 이를 통해 단건 대비 집계 등록 방식이 가지는 비용 효율성을 비교·분석하였다. 본 실험 환경은 실제 운영망을 완전히 재현하기보다는, 제안된 메커니즘의 모듈 단위 성능 특성 및 온체인 연산 효율성을 검증하는 것을 목표로 설계되었다. 또한 본 실험은 Python 기반 프로토타입 환경에서 수행되었기 때문에, 실제 zkSNARK 기반 구현 환경에서는 성능 특성이 달라질 수 있다. 각 실험 결과는 시각화 도구를 활용하여 정량적 비교가 가능하도록 도식화하였다.

4.2 모듈 타당성 분석

본 절에서는 제안된 메커니즘의 프로토타입을 통해 도출된 정량적 결과를 분석한다. 실험은 회로 복잡도별 증명 생성 및 검증 시간, 온체인 가스비, 집계 크기별 비용 효율을 중심으로 수행하였다.

그림 2는 입력 데이터 길이를 회로 복잡도의 근사 지표로 설정하여 증명 생성 및 검증 시간의 변화를 나타낸 것이다. 입력 복잡도는 로그 스케일로 구간을 설정하였으며, 각 구간당 30회 반복 측정을 수행하였다. 결과적으로 복잡도가 증가함에 따라 평균 처리시간은 완만한 상승 곡선을 보였으며, 104이상의 구간에서 급격한 증가가 관찰되었다. 생성과 검증 시간의 차이는 전체 구간에서 0.002ms 수준으로 매우 작게 나타났다. 이는 Python 기반 프로토타입 환경에서 수행된 실험 특성에 따른 결과이다. 이러한 결과는 입력 복잡도가 증가함에 따라 생성 단계와 검증 단계의 처리 시간이 유사한 증가 경향을 보이며, 두 단계 간 연산 부담이 균형적으로 유지됨을 의미한다.

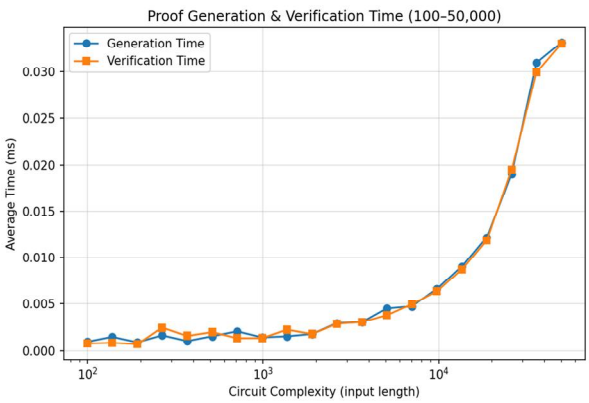


그림 2. 회로 복잡도에 따른 생성/검증 변화
Fig. 2. Generation and verification time by circuit complexity

그림 3은 온체인 정책 등록 과정에서의 배치 크기별 가스 소비량을 보이는 것이다. 평균 가스 사용량은 배치 크기가 1일 때 69274 gas, 50일 때 69284 gas로 측정되어, 전체 구간에서 10 gas 수준의 미세한 상승만을 보였다. 이는 정책 등록 함수가 배치 단위로 병합되어 수행되더라도, 내부 연산의 가스 소비가 선형적으로 증가하지 않음을 의미한다. 단, 본 실험은 로컬 블록체인 테스트 환경에서 수행된 것으로 실제 퍼블릭 블록체인 환경에서는 네트워크 상태 등에 따라 가스 소비 특성이 달라질 수 있다.

그림 4는 가스 소비량의 정규화 효율성 변화를 보이는 것이다. 정규화 효율성 곡선에서는 집계 크기가 커질수록 효율 비율이 완만하게 감소하는 경향이 나타났는데, 이는 개별 트랜잭션 단위의 고정

비가 배치 내에서 분산되어 단건 대비 총비용 효율이 일정 수준에서 수렴함을 보여준다. 따라서 제안된 온체인 구조는 단건 등록 대비 대규모 정책 집계 환경에서 비용 안정성과 처리 효율을 동시에 확보할 수 있는 구조적 특성을 가진다.

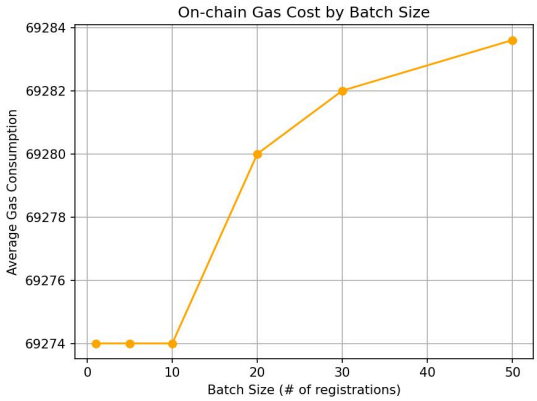


그림 3. 배치 크기에 따른 가스 소비량 변화
Fig. 3. Gas consumption by batch size

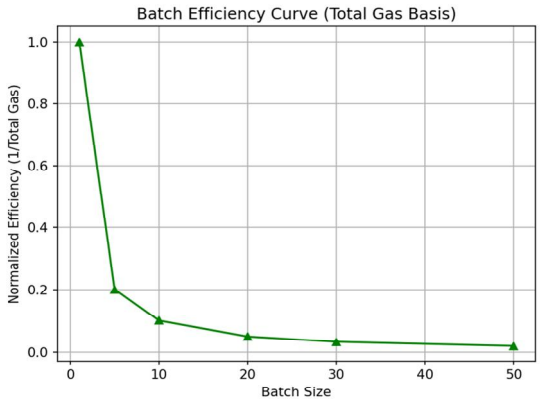


그림 4. 가스 소비량에 따른 정규화 효율성 변화
Fig. 4. Normalized efficiency by gas consumption

4.3 실험 기반 성능 결과 분석

복잡도별 검증 실험 결과, 입력 데이터의 길이를 복잡도의 척도로 설정했을 때 평균 증명 생성 및 검증 시간은 수천 단위까지는 선형 증가를 유지하였으나, 약 5×10^4 구간 이후에는 급격한 상승을 보였다. 이는 단일 회로 내에서 과도한 데이터 처리를 수행할 경우 지연이 누적될 수 있음을 의미한다. 따라서 실시간 처리가 요구되는 환경에서는 회로를 세분화하거나 Fog 단위에서 병렬 증명을 수행하는 방식으로 복잡도를 분산하는 것이 효율적이다.

온체인 트랜잭션 단위에 대한 실험에서는, 배치 크기가 1에서 50으로 증가하더라도 평균 가스 사용량이 69,274 gas에서 69,284 gas로 약 0.014%만 상승하는 것으로 나타났다. 이는 트랜잭션의 집계 단위가 커져도 개별 검증의 비용적 부담이 거의 변하지 않음을 보여준다. 그러나 효율성 곡선 분석 결과, 배치 크기가 1에서 50으로 확대될 때 정규화 효율비는 1.000에서 0.020까지 감소하여, 일정 규모 이상에서는 집계 효율이 점진적으로 포화되는 경향을 보였다. 즉, 배치 크기가 커질수록 총 가스비 대비 효율은 떨어지므로, 5~20건 내외의 소규모 다중 배치 구간이 성능과 비용의 균형점으로 판단된다.

이상의 결과는 복잡도, 처리 단위, 집계 효율이 서로 연동된 지표임을 보여준다. 제안된 구조는 회로 복잡도와 온체인 집계 단위가 일정 수준 이하로 유지될 때 가장 안정적인 성능을 발휘하며, 이는 실제 Fog - Edge 환경에서의 실시간 검증 및 정책 집계에 적용 가능한 설계 기준으로 기능할 수 있다. 다만 본 실험은 로컬 테스트 환경 기반의 프로토타입 구현을 통해 수행되었기 때문에, 실제 대규모 분산 환경에서의 네트워크 지연 및 운영 부하 특성은 추가적인 실험을 통해 검증될 필요가 있다.

V. 결 론

본 논문은 텔레메트리 데이터의 무결성을 중앙 서버에 의존하지 않고 검증하기 위한 새로운 방식으로서, 영지식 증명 기반의 데이터 무결성 검증 메커니즘을 제안하였다. 제안된 구조는 텔레메트리 데이터의 원본 노출 없이 정책 준수 여부를 증명하는 절차를 정의함으로써, 데이터 신뢰성과 프라이버시를 동시에 보장하도록 설계되었다.

이 메커니즘은 종단 장치, 엣지 어그리게이터, 블록체인 네트워크로 구성된 분산 구조 위에서 동작하며, 각 계층의 역할을 명확히 분리하여 연산 효율성과 보안성을 동시에 달성한다. 특히 블록체인 상의 모듈은 정책 버전 관리, 장치 인증, 증명 검증, 결과 기록, 이의 제기 등의 과정을 통합적으로 지원한다. 이러한 구성은 정책 중심의 자율적 데이터 검

증 체계를 가능하게 하며, 기존 중앙집중형 인증 체계의 신뢰 단일점 문제를 해소한다.

또한, 본 논문에서는 모듈 단위 프로토타입을 구현하여 회로 복잡도별 증명 생성·검증 시간, 온체인 가스비, 집계 효율성 등의 성능 지표를 도출하였다. 실험 결과, 제안된 구조는 경량 환경에서도 안정적으로 동작하며, 증명 생성과 검증의 시간 오버헤드가 극히 낮고, 집계 단위 확장 시에도 일정한 비용 효율성을 유지함을 확인하였다. 이를 통해 제안 모델의 구조적 타당성과 실현 가능성을 검증하였다.

향후 연구에서는 정책 변경이나 데이터 이의 제기 상황 등 정책 재검증 및 신뢰 갱신 절차를 포함한 확장 연구를 수행할 예정이다. 이를 통해 블록체인 기반 텔레메트리 데이터 관리 체계가 실시간 보안성, 감사 가능성, 자율성을 모두 갖춘 완전한 형태로 발전할 수 있을 것이다.

References

[1] R. Hu, Z. Yan, W. Ding, and L. T. Yang, "A survey on data provenance in IoT", World Wide Web, Vol. 23, No. 2, pp. 1441-1463, Nov. 2020. https://doi.org/10.1007/s11280-019-00746-1.

[2] J. Kim, N. Park, G. Kim, and S. Jin, "CCTV Video Processing Metadata Security Scheme Using Character Order Preserving-Transformation in the Emerging Multimedia", Electronics, Vol. 8, No. 4, Art No. 412, Apr. 2019. https://doi.org/10.3390/electronics8040412.

[3] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in IoT: challenges and solutions", Blockchain: Research and Applications, Vol. 2, No. 2, Art No. 100006, Jun. 2021. https://doi.org/10.1016/j.bcra.2021.100006.

[4] K. Kent and M. Souppaya, Guide to Computer Security Log Management (SP 800-92), NIST Special Publication, 2006.

[5] J. Kim and N. Park, "Role-based Access Control Video Surveillance Mechanism Modeling in Smart Contract Environment", Transactions on Emerging Telecommunications Technologies, Vol. 33, No. 4, pp. e4227, Feb. 2022. https://doi.org/10.1002/ett.4227.

[6] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized Anonymous Payments from Bitcoin", IEEE Symposium on Security and Privacy, pp. 459-474, Nov. 2014. https://doi.org/10.1109/SP.2014.36.

[7] H. Guo and X. Yu, "A survey on blockchain technology and its security", Blockchain: Research and Applications, Vol. 3, No. 2, Art No. 100067, Jun. 2022. https://doi.org/10.1016/j.bcra.2022.100067.

[8] J. Kim and N. Park, "Suggestions for a Blockchain-based Smart Factory Data Verification Mechanism to Enhance Cloud Data Reliability", Journal of Convergence Science, Technology, and Society, Vol. 2, No. 2, pp. 45-49, Jan. 2023. https://doi.org/10.56366/jcsts.2023.2.2.45.

[9] A. Muñoz, R. Ríos, R. Román, and J. López, "A survey on the (in)security of trusted execution environments", Computers & Security, Vol. 129, Art No. 103180, Jun. 2023. https://doi.org/10.1016/j.cose.2023.103180.

[10] J. Kim and N. Park, "De-Identification Mechanism of User Data in Video Systems According to Risk Level for Preventing Leakage of Personal Healthcare Information", Sensors, Vol. 22, No. 7, Mar. 2022. https://doi.org/10.3390/s22072589.

[11] B. Schneier and J. Kelsey, "Secure Audit Logs to Support Computer Forensics", ACM Transactions on Information and System Security (TISSEC), New York, United States, Vol. 2, No. 2, pp. 159-176, May 1999. https://doi.org/10.1145/317087.317089.

[12] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability", IEEE/ACM CCGrid, Madrid, Spain,

pp. 468-477, May 2017. https://doi.org/10.1109/CCGRID.2017.8.

[13] M. B. Saif, S. Migliorini, and F. Spoto, "A Survey on Data Availability in Layer 2 Blockchain Rollups: Open Challenges and Future Improvements", Future Internet, Vol. 16, No. 9, 315, Aug. 2024. https://doi.org/10.3390/fi16090315.

[14] J. Kim and N. Park, "Blockchain-Based Data-Preserving AI Learning Environment Model for AI Cybersecurity Systems in IoT Service Environments", Applied Sciences, Vol. 10, No. 14, Art No. 4718, Jul. 2020. https://doi.org/10.3390/app10144718.

[15] O. Faraj, D. Megias, and J. Garcia-alfaro, "Security Approaches for Data Provenance in the Internet of Things: A Systematic Literature Review", ACM Computing Surveys, Vol. 57, No. 10, pp. 1-41, May 2025. https://doi.org/10.1145/3718735.

[16] B. Bunz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short Proofs for Confidential Transactions and Mor", 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, May 2018. https://doi.org/10.1109/SP.2018.00020.

[17] J. Groth, "On the Size of Pairing-Based Non-interactive Arguments", Advances in Cryptology – EUROCRYPT 2016, Vienna, Austria, Vol. 9666, pp. 305-326, May 2016. https://doi.org/10.1007/978-3-662-49896-5_11.

[18] M. Maller, S. Bowe, M. Kohlweiss, and S. Meiklejoh, "Sonic:Zero-Knowledge SNARKs from Linear-Size Universal and Updatable Structured Reference Strings", CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London United Kingdom, pp. 2111-2128, Nov. 2019. https://doi.org/10.1145/3319535.3339817.

[19] A. Chiesa, Y. Hu, M. Maller, P. Mishra, N. Vesely, and N. Ward, "Marlin: Preprocessing zkSNARKs with Univeral and Updatable SRS", Advances in Cryptology – EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 2020. https://doi.org/10.1007/978-3-030-45721-1_26.

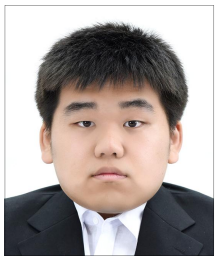
[20] N. Narula, W. Vasquez, and M. Virza, "zkLedger: Privacy-Preserving Auditingfor Distributed Ledgers", NSDI'18: Proceedings of the 15th USENIX Conference on Networked Systems Design and Implementation, Thuwal, Saudi Arabia, pp. 65-80, Apr. 2018.

[21] J. Kim and N. Park, "BlockChain Technology Core Principle Education of Elementary School Student Using Gamification", Journal of The Korean Association of Information Education, Vol. 23, No. 2, pp. 141-148, Apr. 2019.

[22] D. Lee and N. Park, "Technology and Policy Post-Security Management Framework for IoT Electrical Safety Management", The Transactions of The Korean Institute of Electrical Engineers, Vol. 66, No. 12, pp. 1879-1888, Dec. 2017.

저자소개

김 진 수 (Jinsu Kim)



2024년 8월 : 제주대학교 융합정보보안학과(공학박사)
2018년 9월 ~ 현재 : 제주대학교 사이버보안인재교육원 연구원
2025년 11월 ~ 현재 : University of Queensland visiting researcher

관심분야 : 클라우드, 지능형 영상감시 시스템, IoT

최 은 선 (Eunsun Choi)

2022년 8월 : 제주대학교
컴퓨터교육전공(교육학박사)
2020년 3월 ~ 2023년 12월 :
제주대학교
사이버보안인재교육원 연구원
2024년 1월 ~ 2024년 9월 :
요크대학교 물리학, 공학 및
기술학부 박사후연구원
2024년 9월 ~ 현재 : 광주교육대학교 컴퓨터교육과 교수
관심분야 : 인공지능교육, 정보교육, 인공지능 인문학

박 남 제 (Namje Park)

2008년 2월 : 성균관대학교
컴퓨터공학과(공학박사)
2003년 4월 ~ 2008년 12월 : ETRI
정보보호연구단 선임연구원
2009년 1월~ 2010년 8월 : UCLA
Post-Doc., ASU Research
Scientist
2010년 9월 ~ 현재 : 제주대학교 교육대학
초등컴퓨터교육전공 교수,
대학원 융합정보보안협동과정 교수
관심분야 : 융합기술보안, 컴퓨터교육, 스마트그리드, IoT,
해사클라우드