



Sentinel-CTI: A Blockchain-Anchored, Explainable Threat Intelligence Monitoring Framework for Real-Time Cybersecurity

Ritaben Meghajibhai Marwda

Department of Computer Science, Dr. Babasaheb Ambedkar Open University, Ahmedabad, Gujrat, India

Nilesh Modi

Department of Computer Science, Dr. Babasaheb Ambedkar Open University, Ahmedabad, Gujrat, India

Abstract:

Threat intelligence has become the connective tissue of modern cyber defence, yet operational adoption remains constrained by three persistent failures: intelligence is *contextualised knowledge* that must be collected, processed, analysed, and disseminated to the right audience in time to be actionable (Chatziamanetoglou & Rantos, 2023), existing platforms remain *centralised* and carry trust deficits, privacy vulnerabilities, and single points of failure (Tolah, 2025), and monitoring pipelines generate alert volumes that overwhelm analysts – a problem worsened by high false-positive rates and limited contextual understanding in rule-based detection (Kotilingala, 2025). This paper presents Sentinel-CTI, a threat-intelligence monitoring framework that unifies four components: (i) a 26-feature, four-group telemetry schema spanning traffic, behaviour, system-log, and CTI-enrichment signals; (ii) a supervised threat classifier that produces a calibrated threat score fused from model probability, indicator-of-compromise evidence, source reputation, and technique coverage; (iii) an ATT&CK-aligned technique attribution layer that converts raw scores into analyst-readable technique labels, following the demonstrated use of language models for alert classification and technique mapping (Jia et al., 2024; Schärmer, 2026); and (iv) a SHA-256 hash-chained, tamper-evident alert ledger persisted in a relational database, mirroring the provenance guarantees that blockchain-based CTI frameworks provide at consortium scale (Chatziamanetoglou & Rantos, 2024; Preuveneers et al., 2020). The paper contributes a complete, reproducible dataset construction protocol – the Sentinel-CTI corpus, schema-compatible with the publicly available Edge-IIoTset corpus of 1,909,671 samples and 61 traffic features drawn from 1,176 candidate features (Ferrag et al., 2022; Popoola et al., 2023) – together with three executable Python modules covering dataset generation, streaming monitoring with ledger verification, and transformer-based alert triage. All detection metrics reported for Sentinel-CTI are measured on the generated corpus and are explicitly distinguished from deployment-grade evaluation; published systems are used as the comparative baseline set.

Keywords:

Threat Intelligence, Security Monitoring, Blockchain Provenance, ATT&CK Mapping, Intrusion Detection, Explainable Security Analytics, SIEM.