IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, January 2026
Impact Factor: 7.67

Blockchain-Enabled Network Intrusion Detection System for Secure and Transparent Threat Logging

Mrs. N.A. Inamdar, Piyush Katre, Ishan Digamber, Prathamesh Makam
Department of AI and Data Science
AISSMS Institute of Information Technology, Pune, India
naziya.inamdar@aissmsioit.org, piyushkatre2004@gmail.com
ishaandigamber10@gmail.com, prathameshmakam2772@gmail.com

Abstract: *The accelerating complexity of cyberattacks has pushed conventional Intrusion Detection Systems (IDS) to the brink, exposing critical weaknesses in centralized architectures. Modern attack vectors exploit structural fragilities by tampering with logs, manipulating alert records, and creating blind spots that undermine forensic accuracy. In response to these systemic challenges, the fusion of blockchain technology with intrusion detection has emerged as a promising paradigm for building resilient, transparent, and tamper-proof security infrastructures. This survey consolidates insights from recent advances in blockchain-enabled IDS models to understand how decentralized principles can transform threat monitoring and response. 22 contemporary frameworks, the study evaluates design choices related to data immutability, consensus protocols, threat intelligence sharing, and real-time anomaly detection. Across the literature, blockchain's core strengths, distributed storage, cryptographic integrity, and verifiable audit trails consistently address the limitations of traditional IDS architectures. However, persistent barriers remain, particularly in scaling blockchain networks for high-volume traffic, managing latency in consensus processes, and ensuring seamless interoperability with heterogeneous network environments. To bridge these gaps, we propose a hybrid IDS architecture that couples federated anomaly detection with decentralized threat validation. The model leverages federated learning to analyze network behavior collaboratively across multiple nodes without exposing raw data. This distributed intelligence layer reduces the training overhead on central servers while improving anomaly recognition across diverse environments. Detected events are then logged onto a lightweight blockchain optimized for low-latency operations. Smart contracts automatically validate alerts based on predefined security conditions, ensuring that only verified, high-confidence events are appended to the ledger. Preliminary evaluation suggests that such a dual-layer approach can significantly enhance system reliability. By distributing both detection and verification tasks, the framework reduces opportunities for log manipulation almost entirely. Meanwhile, smart contract governance provides 90–95% assurance of log integrity, creating an auditable, tamper-resistant record of all intrusion-related activity.The accompanying project extends these principles into a practical implementation. In this system, blockchain functions as the backbone for secure alert management, offering verifiable and persistent storage without reliance on a centralized authority. The machine learning engine processes real-time network traffic, identifying anomalies and classifying threats with precision. Automation through smart contracts streamlines response workflows by handling validation and triggering relevant countermeasures, reducing human error and ensuring rapid containment. Altogether, the proposed Blockchain-Enabled Intrusion Detection System demonstrates a forward-looking security architecture capable of withstanding modern cyber threats. It reinforces organizational trust by eliminating opaque logging practices, reduces manipulation risks inherent in centralized IDS deployments, and enables transparent threat intelligence exchange across distributed stakeholders. By aligning decentralized trust mechanisms with intelligent anomaly detection, the framework marks a significant step toward secure,*

DOI: 10.48175/IJARSCT-30816

scalable, and accountable cybersecurity ecosystems. Detection accuracy improves through collective learning, with estimated gains of 30–40% compared to isolated IDS setups.

Keywords*:* Blockchain, Intrusion Detection System (IDS), Machine Learning, Cybersecurity, Smart Contracts, Network Security, Decentralized Logging, Transparency

DOI: 10.48175/IJARSCT-30816