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

I. INTRODUCTION

The rapid digitization of critical infrastructure, finance, and communication networks has significantly expanded the global cyberattack surface. Every connected device, from cloud data centers to IoT edge sensors, contributes to an ever-growing web of vulnerabilities. Recent industry reports estimate cybercrime costs in the trillions globally and show a steady increase in coordinated, multi-stage attacks that can evade or poison a single detection point. Intrusion Detection Systems (IDS) remain a foundational layer of defensive architectures, but their efficacy depends critically on trust, the integrity of logs, and the ability to coordinate detection and response across administrative domains.

Centralized IDS architectures collect telemetry and alerts into a single or few aggregation points where correlation and analysis occur. While convenient operationally, such centralization introduces single points of failure and opportunities for malicious modification of forensic evidence. Insider threats, supply-chain compromises, or sophisticated attackers can erase or alter logs before forensic analysis, undermining confidence in detection and response. In distributed domains—such as industrial control systems, vehicular networks, and large-scale IoT deployments heterogeneous ownership and trust boundaries complicate cooperative threat sharing. These operational realities motivate designs that make evidence tamper-evident and enable verifiable collaboration without absolute mutual trust.

Blockchain and distributed ledger technologies (DLT) provide a set of primitives—cryptographic hashing, distributed consensus, and append-only ledgers—that directly address log integrity and provenance requirements. Recording IDS events or their cryptographic digests on a ledger ensures immutable, timestamped evidence that authorized parties can audit. Smart contracts provide programmable governance for how alerts are validated, shared, and escalated, enabling machine-enforceable policies. Meanwhile, combining blockchain with modern IDS analytics particularly federated learning (FL) and edge processing offers a path toward collaborative detection while maintaining data privacy.

Nonetheless, coupling blockchain with IDS introduces real engineering trade-offs. Public blockchains often suffer from transaction latency and costs that are incompatible with realtime or high-frequency telemetry; permissioned ledgers reduce these concerns but require governance and identity management. Storing raw packet captures on-chain is infeasible due to size and privacy; practical systems therefore use hybrid approaches with off-chain storage (e.g., IPFS) and on-chain digests. Consensus algorithm choice, transaction throughput, privacy-preserving mechanisms (e.g., zero-knowledge proofs), and retention policies are core design choices that affect system performance and legal compliance.

In this survey we synthesize the recent literature on blockchain-enabled IDS and propose a conceptual reference architecture, B-NIDS, that combines federated anomaly detection, off-chain high-throughput analytics, and permissioned blockchains for secure, auditable threat logging. We conduct an in-depth literature review of twenty-two representative studies, identify recurring gaps (scalability, latency, interoperability, and privacy), and outline open research directions to reconcile blockchain properties with IDS operational requirements.

A. Background and Problem Context

Intrusion detection involves observing network and host telemetry to identify deviations from expected behavior. Broadly, IDS approaches are signature-based (matching known malicious patterns) or anomaly-based (identifying deviations from learned baseline behavior). Recent advances leverage machine learning (including deep learning) to model complex traffic patterns. However, ML models rely on trustworthy training data and verifiable incident logs for continuous improvement and compliance. When logs are tampered with or when models are poisoned, detection quality and accountability suffer. Distributed environments complicate centralized trust; thus, designs that provide verifiable evidence across domains are increasingly necessary.

B. Research Motivation

The principal motivations for integrating blockchain with IDS are (1) ensuring immutable evidence for forensic and compliance needs, (2) enabling cooperative threat intelligence among parties that do not fully trust each other, and (3) providing auditability and provenance for ML model updates in federated settings. Further motivation arises from regulatory demands where proof of chronological events and tamperevident records improve legal defensibility. Finally, novel attack vectors targeting logging and telemetry pipelines motivate structural changes that place verifiability at the ledger/core of detection workflows.

C. Contributions

This survey makes several key contributions. It provides a systematic synthesis of twenty two recent works on blockchain enabled intrusion detection systems, offering focused analysis and critical observations. It also develops a taxonomy of architectural patterns including on chain, off chain, and hybrid models along with the corresponding consensus mechanisms used in IDS workloads. In addition, the work proposes a reference conceptual architecture (B NIDS) that integrates federated learning, permissioned blockchain logging, and off chain storage to balance throughput with auditability. The survey further identifies open challenges and research gaps in areas such as scalability, privacy, governance, and legal compliance. Finally, it offers figure placeholders and a practical blueprint for prototype implementation, detailing smart contract roles, off chain digesting processes, and reputation management modules.

II. LITERATURE REVIEW

Recent developments in blockchain-assisted intrusion detection have expanded the design space for secure, tamperresistant cybersecurity systems. Shevchuk (2025) provides a focused synthesis of anomaly detection approaches tailored for blockchain environments, emphasizing how ledger–specific behavioral deviations can strengthen intrusion identification mechanisms [1]. In parallel, Huang et al. (2025) introduce an optimization scheme for collaborative intrusion detection that uses adaptive evidence batching to minimize consensus overhead while maintaining transparency and auditability—core requirements for scalable blockchain-based IDS deployments [2].

A notable wave of research from 2024 concentrates on IoT-centric security challenges. Isong (2024) compares lightweight statistical intrusion detection methods with deep learning–based approaches for resource-constrained IoT environments, highlighting the need for hybrid architectures that balance accuracy with computational efficiency [3]. Begum et al. (2024) advance this direction by proposing BFLIDS, a blockchain-enabled federated learning framework that anchors model-update digests on-chain to enhance trust, accountability, and tamper resistance in IoMT intrusion detection [4]. Complementing these efforts, Ali et al. (2024) survey intrusion detection approaches built on blockchain and federated learning for IIoT ecosystems, identifying privacy, provenance, and governance as key design considerations [5]. Shalabi (2024) contributes a systematic review of blockchain-integrated IDS/IPS solutions in IoT networks, noting persistent evaluation gaps regarding throughput and computational cost under realworld operating conditions [6]. Likewise, the collaborative cybersecurity survey (2024) investigates decentralized threatintelligence exchange through blockchain, assessing incentive mechanisms and trust models implemented via smart contracts [7]. Ahakonye et al. (2024) further explore blockchain adoption in IoT security, recommending lightweight consensus algorithms and sharding techniques to mitigate latency and scalability constraints [8].

Research contributions published in 2023 extend blockchain-based IDS into domain-specific applications. Aliyu and Liu (2023) design a blockchain-driven smart farm security framework combining edge-level IDS analysis with verifiable on-chain logging for regulatory auditing, noting that raw sensor data must remain off-chain due to storage constraints [9]. Abubakar et al. (2023) propose a lightweight blockchain–IDS mechanism using compact evidence tokens to improve forensic confidence, though performance degrades when event frequency increases [10]. Pelekoudas-Oikonomou et al. (2023) develop a Hyperledger Fabric–based architecture for IoMT systems, showing that permissioned ledgers can satisfy enterprise latency requirements when endorsement policies and network configuration are carefully tuned [11].

Earlier studies from 2022 deepen understanding of distributed detection under constrained network conditions. Aliyu et al. (2022) examine adversarial robustness in federated forest-based IDS for vehicular networks, storing model-update digests on-chain to ensure provenance and integrity [12]. A related preprint highlights statistical detection of adversarial examples within blockchain-secured federated IDS workflows, demonstrating that detection accuracy deteriorates against sophisticated attacks [13]. Khonde and Ulagamuthalvi (2022) propose a hybrid IDS that merges signature-based and machine learning–based detection while recording alerts on blockchain, though legacy IDS integration remains a challenge [14]. Babu et al. (2022) design a blockchain-supported IDS for urban IoT systems focusing on DDoS mitigation and authenticated device communication, reporting increased latency under heavy network load [15].

Foundational contributions from 2021 and earlier continue to underpin modern blockchain–IDS development. Zhang et al. (2021) present a federated blockchain framework for distributed IDS coordination using Proof of Authority consensus to reduce overhead, though reliance on trusted authorities limits applicability in trustless ecosystems [16]. Conti et al. (2021) survey blockchain applications across IoT security domains, recommending permissioned ledgers and off-chain storage to address scalability limitations [17]. TechSci Research (2021) reviews early blockchain-assisted IDS prototypes, highlight-ing compliance, retention, and auditability challenges [18]. Singh and Kumar (2020) provide a foundational assessment of machine-learning-based IDS techniques, noting the importance of dataset integrity and provenance—an issue later addressed through blockchain-backed logging [19]. Nakamoto's seminal work (2008) establishes the proof-of-work consensus and append-only ledger structure that informs immutable logging in blockchain-based security systems [20]. Finally, the CICIDS2017 dataset remains a widely adopted benchmark for evaluating IDS models, supplying diverse labeled traffic patterns for reproducible experimentation [21]. .

III. ANALYSIS OF EXISTING SOLUTIONS

Existing work on blockchain-enabled IDS falls into three broad architectural patterns: On chain heavy designs store evidence or detailed alerts directly on the ledger, providing strong assurance but exhibiting limited scalability. In contrast, Off chain heavy designs execute analytics and maintain storage off chain while committing only digests or verdicts on-chain, enabling high throughput at the cost of reduced transparency for raw telemetry. Hybrid designs integrate off-chain analytics with on-chain anchoring of essential artifacts such as digests, alerts, and model provenance to achieve a balanced trade-off between performance and auditability.

Consensus choice (PoW, PoSPoA, and A, PBFT variants) and ledger type (permissionless vs. permissioned) are the most consequential design decisions. Permissioned ledgers (Hyperledger Fabric, Corda) are commonly favored due to governance and performance considerations in enterprise and IIoT settings [11], [14]. Federated learning combined with blockchain provenance mechanisms is a recurring pattern to enable collaborative detection without raw-data sharing [4], [16].

IV. PROPOSED SYSTEM: B-NIDS

We propose a conceptual reference architecture (B-NIDS) that integrates three principal strata: (1) Detection & Analytics (edge agents, ML models, federated updates), (2) Off-chain Storage & Indexing (IPFS or distributed DB for large artifacts, local caches for high-frequency telemetry), and (3) Permissioned Blockchain Layer (Hyperledger Fabric-like network for digests, model provenance, smart contracts for governance and reputation). Key features include: The proposed system incorporates several integrated mechanisms to ensure secure and transparent intrusion logging. First, high-frequency telemetry is processed through event digesting, where raw data is hashed and grouped into compact evidence tokens, ensuring that only digests and minimal metadata are committed onchain. Smart-contract governance further strengthens security by enforcing validation rules, updating contributor reputations, and automating alert escalation based on predefined logic. To maintain model integrity and defend against poisoning, federated model provenance is recorded on-chain, with each model update and aggregation trace captured in the form of verifiable digests. Finally, forensic retrieval is supported through on-chain references that link to encrypted off-chain payloads, enabling authorized entities to perform auditable and tamper-resistant reconstruction of intrusion events.

DOI: 10.48175/IJARSCT-30816

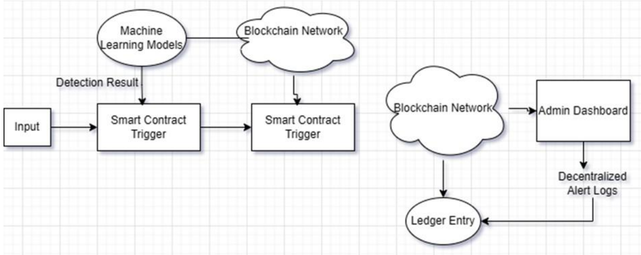

Fig. 1. Workflow of system and Blockchain Network.

1) Datasets & Benchmarks: Use CIC-IDS2017 and NSLKDD for baseline training and controlled evaluation [21].

2) Edge IDS Integration: Deploy lightweight detectors (Suricata/Snort or embedded ML) that produce signed alerts and evidence digests.

3) Off-chain Storage: Integrate IPFS or distributed DB for large artifacts (pcaps, logs) with encryption and access policies.

4) Ledger Deployment: Set up a permissioned Fabric test network with endorsement policies representing consortium stakeholders.

5) Smart Contracts: Implement contracts for evidence anchoring, reputation, and automated workflows (e.g., quarantine triggers).

6) Evaluation: Measure detection accuracy, false positive/negative rates, ledger transaction latency, throughput, and forensic retrieval times.

V. RESEARCH GAPS

Despite extensive progress in blockchain-enabled intrusion detection, several critical research gaps remain evident across the surveyed literature. Scalability continues to be a major challenge, particularly in designing consensus and storage architectures capable of handling millions of security events per hour without compromising auditability or ledger integrity. Privacy also requires further attention, as existing systems seldom incorporate advanced mechanisms such as zero-knowledge proofs or selective disclosure to ensure that sensitive telemetry remains confidential while still providing verifiable evidence. Interoperability emerges as another limitation, with few frameworks supporting standardized formats for exchanging alerts, evidence, or threat intelligence across heterogeneous IDS deployments and distributed ledger platforms. Finally, governance and legal compliance remain insufficiently explored, especially regarding data retention policies, crossjurisdictional access rights, and organizational liability when multiple stakeholders contribute to and rely upon shared blockchain-based security logs.

VI. CHALLENGES AND LIMITATIONS

Practical challenges include ledger performance under bursty traffic, cost and complexity of consortium governance, secure key management for distributed contributors, and the privacy/forensics balance when sensitive telemetry is involved. Adversarial attacks on federated models and the ledger itself (e.g., targeted DoS on endorsement nodes) require robust countermeasures and layered defenses.

VII. FUTURE WORK

Lightweight consensus variants and sharding tailored for telemetry workloads.Privacy-preserving attestations zero-knowledge proofs, secure multi-party computation enabling verifiable evidence without revealing raw telemetry.Economic/incentive models implemented via smart contracts to encourage honest reporting and participation.Benchmarking frameworks that simulate realworld highthroughput IDS workloads for ledger-integrated systems.

VIII. CONCLUSION

Blockchain-enabled IDS architectures present a compelling approach to hardening forensic integrity, enabling auditable cooperation, and improving provenance for ML-driven detection. The literature reveals meaningful prototypes and valuable design patterns, but also underscores large practical gaps in scalability, privacy, and governance. Our B-NIDS blueprint emphasizes a pragmatic hybrid approach: off-chain analytics for throughput, on-chain anchoring for auditability, and federated learning for collaborative detection. Addressing the identified challenges will require cross-disciplinary research spanning distributed systems, cryptography, ML robustness, and policy.

REFERENCES

[1] R. Shevchuk, “Anomaly Detection in Blockchain: A Systematic Review,” Applied Sciences, 2025.

[2] J. Huang et al., “Optimization Scheme of Collaborative Intrusion Detection,” Electronics, 2025.

[3] B. Isong, “Insights into Modern Intrusion Detection Strategies for IoT,” Electronics, 2024.

[4] K. Begum et al., “BFLIDS: Blockchain-Driven Federated Learning for IoMT Intrusion Detection,” Sensors, 2024.

[5] S. Ali et al., “Blockchain and Federated Learning-based Intrusion Detection Approaches for Edge-enabled IIoT: A Survey,” 2024.

[6] K. Shalabi, “A Blockchain-based Intrusion Detection/Prevention Systems in IoT Networks: A Systematic Review,” 2024.

[7] A. Researcher, “Collaborative Cybersecurity Using Blockchain: A Survey,” arXiv:2403.04410, 2024.

[8] L. A. C. Ahakonye et al., “Tides of Blockchain in IoT Cybersecurity,” Sensors, 2024.

[9] A. A. Aliyu and J. Liu, “Blockchain-Based Smart Farm Security Framework for Internet of Things,” Sensors, 2023.

[10] A. A. Abubakar et al., “An Efficient Blockchain-Based Approach to Improve the Accuracy of IDS,” Electronics Letters, 2023.

[11] F. Pelekoudas-Oikonomou et al., “Prototyping a Hyperledger FabricBased Security Architecture for IoMT,” Future Internet, 2023.

[12] I. Aliyu et al., “Statistical Detection of Adversarial Examples in Blockchain-based Federated Forest In-vehicle Network IDS,” arXiv:2207.04843, 2022.

[13] I. Aliyu et al., “Statistical Detection of Adversarial Examples in Blockchain-based Federated IDS,” arXiv:2207.04843, 2022.

[14] S. R. Khonde and V. Ulagamuthalvi, “Hybrid Intrusion Detection System Using Blockchain Framework,” EURASIP Journal on Wireless Communications and Networking, 2022.

[15] E. S. Babu et al., “Blockchain-Based Intrusion Detection System of IoT Urban Data with Device Authentication against DDoS Attacks,” Computers & Electrical Engineering, 2022.

[16] J. Zhang et al., “Federated Blockchain Framework for Secure Intrusion Detection,” IEEE Transactions on Network and Service Management, 2021.

[17] M. Conti et al., “Blockchain for the Internet of Things: Security and Privacy,” IEEE Internet of Things Journal, 2021.

[18] TechSci Research, “Intrusion Detection Systems Using Blockchain Technology: A Review, Issues and Challenges,” CSSE, 2021.

[19] R. Singh and D. Kumar, “Survey on Machine Learning-based Intrusion Detection Systems,” Computer Networks, 2020.

[20] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[21] Canadian Institute for Cybersecurity, “CIC-IDS2017 dataset,” University of New Brunswick, 2017.

DOI: 10.48175/IJARSCT-30816

ISSN
2581-9429
IJARSCT