International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Role of Blockchain Technology in Intrusion Detection Systems: A Comprehensive Review and Future Directions

Shaina Mahajan[1], Parveen Sadotra[2], Kailash Thakur[3]

[1,3]Research Scholar, Department of Computer Science and Informatics, Central University of Himachal Pradesh
[2]Assistnat Professor, Department of Computer Science and Informatics, Central University of Himachal Pradesh
[2]*Corresponding Author Email: Sadotramca2k6@gmail.com*

Abstract
Intrusion Detection Systems (IDS) are foundational components of modern network security infrastructure. Despite decades of advancement, conventional IDS architectures remain vulnerable to single points of failure, data tampering, lack of transparency, and insufficient collaboration across organisational boundaries. Blockchain technology, with its inherent properties of decentralisation, immutability, transparency, and consensus-based trust, offers a compelling framework to address these longstanding limitations. This paper presents a comprehensive review of the integration of blockchain technology with IDS architectures, examining the fundamental principles, architectural paradigms, state-of-the-art proposals, and practical implementations reported in the literature. We analyse how blockchain enhances IDS across four critical dimensions: data integrity and tamper-resistance of alert logs, decentralised and collaborative threat intelligence sharing, smart-contract-driven automated response mechanisms, and privacy-preserving detection frameworks. We further discuss key challenges including scalability, latency, storage overhead, and consensus mechanism selection. Finally, we identify open research directions and propose a unified blockchain-IDS reference architecture suitable for heterogeneous network environments including IoT, cloud, and Software-Defined Networks (SDN).

Keywords: Blockchain, Intrusion Detection System (IDS), Network Security, Decentralised Trust, Smart Contracts, Threat Intelligence, Immutability, Distributed Ledger Technology (DLT), Cyber Threat Sharing, IoT Security.

1. INTRODUCTION

The rapid expansion of digital infrastructure, the proliferation of Internet-connected devices, and the increasing sophistication of cyber threats have collectively elevated network security to a matter of critical national and organisational importance. Intrusion Detection Systems (IDS) constitute one of the most fundamental defensive mechanisms deployed within this security landscape. An IDS monitors network traffic and system activities, identifies suspicious behaviour, and generates alerts for human analysts or automated response systems [1]. Despite their centrality to security operations, traditional IDS

architectures suffer from a cluster of well-documented structural vulnerabilities that significantly constrain their effectiveness.

Chief among these vulnerabilities is the centralised architecture that most conventional IDS platforms employ. A centralised IDS creates a single point of failure: if the detection node is compromised, disabled, or simply overwhelmed by volumetric attacks, the entire detection capability of the defended network may collapse. Furthermore, the event logs and alert records generated by an IDS are typically stored in databases that, if accessed by a sophisticated adversary, can be altered or deleted to conceal evidence of an intrusion. The tamper-resistance of forensic evidence is thus a fundamental concern in IDS design [2].

A second major limitation is the siloed nature of threat intelligence in most organisational deployments. Each enterprise operates its own IDS largely independently, sharing little or no detection data with peer organisations. This isolation means that novel attack patterns observed in one organisation's network may not be known to others until the attack propagates. Mechanisms for trusted, privacy-preserving threat intelligence sharing remain underdeveloped in practice, largely because of concerns about data confidentiality and the absence of a trusted intermediary [3].

Blockchain technology—a form of Distributed Ledger Technology (DLT)—has attracted considerable research interest as a potential solution to these challenges. A blockchain is a shared, append-only ledger in which records are grouped into cryptographically linked blocks and replicated across a peer-to-peer network. Once a record is committed to the chain, modifying it requires recomputing the proof-of-work (or equivalent consensus evidence) for all subsequent blocks, which is computationally infeasible in a sufficiently large network. This immutability, combined with the decentralised replication of the ledger and the programmability offered by smart contracts, makes blockchain a compelling infrastructure layer for IDS [4].

This paper makes the following contributions: (i) a structured taxonomy of blockchain-IDS integration architectures; (ii) a comprehensive survey of existing proposals, classified by their primary contribution; (iii) a comparative analysis of consensus mechanisms and their suitability for IDS contexts; (iv) a discussion of open research challenges; and (v) a proposed reference architecture for blockchain-enhanced IDS in heterogeneous environments.

2. BACKGROUND AND RELATED WORK

2.1 Intrusion Detection Systems: Fundamentals

An IDS can be broadly categorised along two orthogonal dimensions: deployment location and detection methodology. With respect to deployment, a Network-based IDS (NIDS) monitors traffic traversing a network segment, while a Host-based IDS (HIDS) monitors events on a specific host—system calls, file access patterns, process behaviour. Hybrid IDS architectures combine both modalities to achieve broader coverage [5].

With respect to detection methodology, Signature-based IDS (also called misuse-detection IDS) maintains a database of known attack signatures and raises alerts when observed traffic or behaviour matches a signature. While highly accurate for known attacks, signature-based detection is blind to zero-day exploits and novel attack variants. Anomaly-based IDS, by contrast, builds a statistical model of normal behaviour

and flags deviations from the baseline as potential intrusions. Anomaly detection can identify novel attacks but tends to produce higher false positive rates [6]. Specification-based and hybrid detection approaches occupy intermediate positions.

Deep learning and machine learning (ML) have dramatically expanded the detection capability of anomaly-based IDS in recent years. Architectures including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM) networks, and Transformer-based models have been applied to intrusion detection with state-of-the-art performance on benchmark datasets such as KDD Cup 99, NSL-KDD, CICIDS, and UNSW-NB15 [7]. Nevertheless, these ML advances have not resolved the structural architectural limitations of centralisation and lack of trustworthy data sharing.

2.2 Blockchain Technology: Core Principles

Blockchain was first articulated by Nakamoto in the seminal Bitcoin whitepaper of 2008 as a peer-to-peer electronic cash system secured by a Proof-of-Work (PoW) consensus mechanism [8]. Since then, the technology has evolved significantly. The key properties of a blockchain relevant to IDS applications are as follows.

Decentralisation: No single node controls the ledger; records are replicated across all participating nodes, eliminating single points of failure.

Immutability: Once a block is confirmed and appended to the chain, altering its contents requires invalidating all subsequent blocks—a computationally prohibitive task in a sufficiently large network.

Transparency: All participants can independently verify the contents of the ledger, enabling auditable and accountable record-keeping.

Smart Contracts: Self-executing programs stored on the blockchain that automatically enforce predefined rules when specified conditions are met, enabling trustless automation of complex workflows.

Consensus Mechanisms: Protocols (e.g., Proof-of-Work, Proof-of-Stake, Practical Byzantine Fault Tolerance) by which distributed nodes agree on the current state of the ledger without requiring a central authority.

Public blockchains (e.g., Ethereum) are open to any participant but face scalability constraints. Private (permissioned) blockchains (e.g., Hyperledger Fabric) restrict participation to vetted nodes, offering higher throughput and lower latency at the cost of reduced decentralisation—a trade-off particularly relevant to IDS deployments where performance requirements are stringent [9].

2.3 Related Work Overview

Research at the intersection of blockchain and IDS has grown substantially since approximately 2017. Golomb et al. [10] proposed BitcoinHEX, one of the earliest blockchain-based threat intelligence sharing frameworks. Golomb's work demonstrated that the immutable, decentralised nature of blockchain could serve as a trustworthy repository for Indicators of Compromise (IoC). Subsequent work by Alexopoulos et al. [11] formalised a taxonomy of blockchain-assisted security information sharing and identified key privacy challenges.

Li et al. [12] presented a consortium blockchain architecture for collaborative IDS in which IDS nodes across multiple organisations contribute alert data to a shared ledger, while smart contracts enforce data quality and access control policies. Meng et al. [13] surveyed blockchain-based IoT security frameworks and identified IDS as a key beneficiary of blockchain integration. More recent works have incorporated federated learning into blockchain-IDS frameworks to achieve privacy-preserving collaborative model training [14].

Key Observation: The literature consistently identifies three primary motivations for blockchain-IDS integration: (1) tamper-proof audit trails, (2) decentralised threat intelligence sharing, and (3) automated smart-contract-driven response.

3. BLOCKCHAIN-IDS INTEGRATION: ARCHITECTURAL PARADIGMS

The integration of blockchain with IDS can be realised through several distinct architectural paradigms, each addressing a different subset of the limitations described in Section 1. We identify and analyse four primary paradigms.

3.1 Blockchain as Tamper-Proof Alert Storage

In this paradigm, the IDS operates conventionally—monitoring traffic, applying detection logic, generating alerts—but instead of writing alert records to a centralised database, it hashes each alert and submits the hash (or the full alert record, depending on privacy requirements) as a transaction to a blockchain. The blockchain then serves as an immutable audit log of all detection events.

The primary security benefit is forensic integrity. If an attacker compromises the IDS host and attempts to delete or modify alert records, the on-chain hashes immediately reveal the discrepancy. Legal admissibility and auditability of incident records are significantly enhanced. Since only hashes need be stored on-chain, storage overhead is manageable, and sensitive payload data can be retained off-chain while still being cryptographically bound to the ledger [15].

3.2 Decentralised Collaborative Threat Intelligence Sharing

This paradigm extends the blockchain layer beyond a single organisation to form a consortium or federated network of IDS nodes. Each node monitors its own network segment and contributes Indicators of Compromise (IoCs)—malicious IP addresses, file hashes, domain names, attack signatures—to a shared blockchain. Smart contracts govern the submission process, enforcing validation rules, rewarding high-quality contributions (via token incentives in some schemes), and providing access control to ensure that only vetted participants can read sensitive data [16].

The key challenge here is the tension between sharing and confidentiality. Organisations are often reluctant to share threat data that might reveal information about their internal vulnerabilities or ongoing incidents. Privacy-preserving techniques—zero-knowledge proofs, homomorphic encryption, and secure multi-party computation—have been proposed to enable sharing of actionable intelligence without exposing sensitive contextual details [17].

3.3 Smart-Contract-Driven Automated Response

Smart contracts on the blockchain can be programmed to trigger automated responses when detection conditions are met. For instance, if a certain threshold of participating IDS nodes concurrently report traffic from the same source IP as malicious, a smart contract can automatically issue a blocking rule that is distributed to all network enforcement points (firewalls, routers, SDN controllers). This enables a consensus-based, decentralised intrusion response that does not depend on a central command server [18].

This paradigm is particularly valuable in SDN environments, where the blockchain can interact directly with the SDN controller via smart contracts to dynamically update flow tables in response to detected intrusions. The immutability of the contract execution record provides an auditable history of all automated responses, facilitating post-incident analysis [19].

3.4 Blockchain-Federated Learning Hybrid IDS

The most recent paradigm combines federated machine learning with blockchain infrastructure. In a federated IDS, each participating organisation trains a local ML detection model on its own data, and the model updates (gradients or weights) rather than the raw data are shared. The blockchain is used to record and version-control model updates, detect and exclude malicious participants who submit poisoned gradients (a form of Byzantine fault), and provide a transparent, auditable history of the global model's evolution [20].

This paradigm addresses both the privacy concern—raw traffic data never leaves the organisation—and the integrity concern—the immutable blockchain record prevents a malicious coordinator from silently manipulating the aggregated model. It represents the current frontier of blockchain-IDS research.

4. COMPARATIVE ANALYSIS

4.1 Comparison of Blockchain Types for IDS Applications

Table 1 summarises the suitability of different blockchain types for IDS integration across key evaluation criteria.

Criterion	Public Blockchain	Private Blockchain	Consortium Blockchain
Decentralisation	Very High	Low	Medium
Throughput (TPS)	Low (7–30)	High (1000+)	Medium (200–1000)
Latency	High (minutes)	Low (seconds)	Low–Medium
Privacy Control	Minimal	Full	Configurable
Trust Model	Trustless	Trusted Nodes	Semi-trusted
Smart Contracts	Yes (Ethereum)	Yes (Fabric)	Yes
Cost	High (gas fees)	None	Minimal
IDS Suitability	Low–Medium	High	Very High

Table 1: Comparison of blockchain types for IDS integration

4.2 Consensus Mechanisms and Their Suitability

Table 2 compares major consensus mechanisms with respect to criteria most relevant to IDS deployments.

Mechanism	Fault Tolerance	Throughput	Finality	Best IDS Context

Proof of Work (PoW)	< 50% hash power	Very Low	Probabilistic	Not recommended
Proof of Stake (PoS)	< 33% stake	Medium	Probabilistic	Public threat logs
PBFT	< 33% Byzantine	High	Immediate	Enterprise / SDN IDS
Raft / CFT	< 50% crash	Very High	Immediate	Intra-org HIDS
Tendermint	< 33% Byzantine	High	Immediate	Consortium IDS
PoA / Clique	Trusted validators	Very High	Immediate	Private IDS networks

Table 2: Consensus mechanisms and suitability for IDS applications

5. DOMAIN-SPECIFIC APPLICATIONS

5.1 Blockchain-IDS for IoT Networks

The Internet of Things presents a uniquely challenging environment for IDS deployment. IoT devices are often resource-constrained—limited CPU, memory, and battery capacity—making it impractical to run traditional IDS software directly on the device. Furthermore, IoT networks are highly heterogeneous and may span millions of devices across geographically dispersed deployments. The conventional approach of routing all traffic through a centralised IDS creates bottlenecks and single points of failure that attackers can exploit [21].

Blockchain-based IoT IDS architectures typically adopt a lightweight edge-based detection model in which IDS processing is offloaded to edge gateways with more resources. These gateways submit compressed detection results or IoC hashes to a permissioned blockchain. Smart contracts aggregate reports from multiple gateways and trigger responses when consensus thresholds are exceeded. Lightweight consensus mechanisms such as Proof of Authority (PoA) or Delegated Proof of Stake (DPoS) are preferred to minimise latency and energy consumption [22].

A notable proposal in this space is the work of Hossain et al. [23], who designed a blockchain-based NIDS for smart home IoT environments. Their architecture uses a Raspberry Pi-class edge device as the local IDS agent, submitting detection events to a private Ethereum blockchain. Evaluation showed detection accuracy comparable to centralised alternatives with significantly improved resilience to node compromise attacks.

5.2 Blockchain-IDS in Cloud Environments

Cloud environments introduce additional challenges including multi-tenancy, dynamic resource allocation, and the geographic distribution of workloads across multiple data centres. Virtual Machine (VM) migration and the rapid provisioning and decommissioning of instances create gaps in intrusion detection coverage. Furthermore, cloud tenants typically cannot audit the security of shared infrastructure [24].

Blockchain-based cloud IDS architectures address these challenges by maintaining an immutable record of VM lifecycle events, network flow summaries, and IDS alerts on a consortium blockchain shared among cloud providers and their customers. Smart contracts enforce Service Level Agreements (SLAs) related to security, automatically logging violations and triggering compensatory actions. Qin et al. [25] demonstrated a prototype on Hyperledger Fabric with a throughput of 850 TPS and a detection latency of under 2 seconds, meeting real-time requirements for most cloud security use cases.

5.3 Blockchain-IDS in Software-Defined Networks (SDN)

SDN separates the control plane from the data plane, centralising network intelligence in one or more SDN controllers. While this centralisation enables programmable, flexible network management, it also creates a high-value target for attackers: compromising the SDN controller effectively gives an adversary control of the entire network [26].

Integrating blockchain with SDN-based IDS decentralises the control plane trust: multiple SDN controllers share a blockchain ledger of flow rules and policy decisions. Any controller that issues an anomalous flow rule—potentially indicating compromise—can be detected and overruled by consensus. Smart contracts implement the detection and response logic, ensuring that no single compromised controller can unilaterally install malicious flow rules [27].

6. CHALLENGES AND OPEN RESEARCH PROBLEMS

6.1 Scalability and Performance

Throughput and latency remain the most pressing practical challenges for blockchain-IDS integration. An IDS operating on a high-speed enterprise network may generate thousands of alerts per second. Committing each alert as a blockchain transaction is infeasible for most consensus mechanisms. Proposed mitigations include: (i) batching multiple alerts into a single transaction using Merkle trees; (ii) storing only cryptographic hashes on-chain with full data in off-chain storage (IPFS or encrypted cloud storage); and (iii) using Layer-2 solutions or state channels for high-frequency interactions with periodic settlement to the main chain. Research quantifying the performance overhead of these approaches under realistic IDS workloads remains limited [28].

6.2 Privacy and Data Confidentiality

While the transparency of the blockchain is a security asset, it conflicts with organisations' requirements to keep threat data confidential. Publishing IoCs publicly may reveal internal network topology or ongoing incident response activities to adversaries. Zero-knowledge proof systems—particularly zk-SNARKs (Zero-Knowledge Succinct Non-interactive Arguments of Knowledge)—allow a node to prove that it has observed a certain attack pattern without revealing the raw data [29]. However, the computational overhead of zk-SNARK generation is substantial, and integrating these proofs into real-time IDS workflows is an active area of research.

6.3 Smart Contract Vulnerabilities

Smart contracts, once deployed, are immutable and execute exactly as programmed. If a contract contains a vulnerability—as demonstrated by the infamous DAO hack on Ethereum in 2016—it can be exploited to subvert the very security mechanisms it was intended to provide. Formal verification of smart contracts using tools such as K-framework or Certora Prover is essential but is not yet standard practice in blockchain-IDS systems. The complexity of detection and response logic exacerbates this risk [30].

6.4 Sybil Attacks and Poisoning

In a collaborative blockchain-IDS network, a malicious participant can register multiple fake identities (Sybil attack) and flood the ledger with false IoCs, causing benign traffic to be flagged as malicious (a form of data poisoning). Reputation systems and stake-based admission control partially mitigate this risk, but robust, attack-resistant identity management for large-scale blockchain IDS deployments remains an open problem [31].

6.5 Interoperability and Standardisation

The lack of standard data formats for blockchain-exchanged threat intelligence is a significant barrier to adoption. While frameworks such as STIX (Structured Threat Information Expression) and TAXII (Trusted Automated eXchange of Indicator Information) provide some standardisation for threat intelligence sharing, their integration with blockchain transaction formats is not standardised. Cross-chain interoperability—enabling consortium chains operated by different organisations or industries to exchange data—requires bridge protocols that introduce new trust assumptions [32].

Research Gap: A unified standard for blockchain-encoded intrusion detection data—covering transaction formats, smart contract interfaces, and cross-chain communication protocols—is urgently needed to enable large-scale, multi-organisational blockchain-IDS deployments.

7. PROPOSED REFERENCE ARCHITECTURE

Drawing on the analysis in preceding sections, we propose a five-layer reference architecture for blockchain-enhanced IDS, designed to be applicable to heterogeneous network environments including enterprise, IoT, cloud, and SDN deployments. The layers are described as follows.

Layer 1 — Detection Layer: Distributed IDS agents (NIDS/HIDS) deployed at network segments, hosts, and edge gateways. Agents use ML-based anomaly detection supplemented by signature matching. Lightweight agents are designed for resource-constrained IoT devices; full-featured agents operate on enterprise hosts and cloud instances.

Layer 2 — Preprocessing and Aggregation Layer: Detected events are preprocessed: normalised to a standard format (STIX-compatible), deduplicated, correlated across agents, and aggregated using Merkle trees to produce compact, verifiable summaries suitable for blockchain submission.

Layer 3 — Blockchain Ledger Layer: A consortium permissioned blockchain (Hyperledger Fabric-based) operated by vetted organisational nodes. PBFT or Tendermint consensus ensures immediate finality. Alert summaries, IoC hashes, and model update commitments are stored as transactions. Off-chain storage (IPFS with content addressing) holds full alert records linked by on-chain hashes.

Layer 4 — Smart Contract Logic Layer: Deployed smart contracts implement: (a) IoC submission and validation; (b) reputation scoring of contributing nodes; (c) consensus-based alert escalation; (d) automated response trigger logic; (e) federated learning model update aggregation and Byzantine filtering.

Layer 5 — Response and Enforcement Layer: Automated responses orchestrated by smart contracts propagate to network enforcement points: firewall rule updates, SDN flow table modifications, user account suspension, and incident ticket creation. A human analyst dashboard provides real-time visibility into the blockchain-recorded security posture.

The architecture decouples detection capability from trust infrastructure: detection agents can be upgraded or replaced without modifying the blockchain layer, and the blockchain provides a stable, auditable substrate regardless of changes to the detection methodology. This modularity is a key advantage over monolithic IDS architectures.

8. FUTURE RESEARCH DIRECTIONS

- Quantum-resistant blockchain cryptography: Current blockchain security relies on elliptic curve cryptography vulnerable to quantum attacks. Post-quantum signature schemes (lattice-based, hash-based) must be integrated into blockchain-IDS frameworks ahead of the practical availability of quantum computers.

- Real-time blockchain transaction processing: Developing ultra-low-latency consensus mechanisms capable of processing IDS alert transactions in sub-100ms, suitable for time-sensitive intrusion response in critical infrastructure environments.

- AI-driven smart contract generation: Automatically synthesising formally verified smart contracts from high-level security policy specifications, reducing the engineering burden and smart contract vulnerability risk.

- Privacy-preserving threat sharing with zk-SNARKs: Implementing production-grade zero-knowledge proof systems for IoC sharing that are efficient enough for real-time IDS workflows on commodity hardware.

- Blockchain-IDS for 5G and edge computing: Extending blockchain-IDS frameworks to 5G network slices and mobile edge computing environments, where the extremely low latency requirements and massive device counts pose new challenges.

- Cross-chain federated IDS: Enabling IDS collaboration across organisations operating different blockchain platforms through interoperability bridges with formal security guarantees.

9. CONCLUSION

This paper has presented a comprehensive examination of the role of blockchain technology in enhancing Intrusion Detection Systems. We have demonstrated that the core properties of blockchain—decentralisation, immutability, transparency, and programmability through smart contracts—directly address the most significant structural weaknesses of conventional IDS architectures: centralised single points of failure, tamper-vulnerable alert records, and the absence of trusted, privacy-respecting mechanisms for cross-organisational threat intelligence sharing.

Through a structured survey of existing proposals, we have identified four principal integration paradigms: blockchain as tamper-proof alert storage, decentralised collaborative threat intelligence sharing, smart-contract-driven automated response, and blockchain-federated learning hybrid IDS. Each paradigm offers distinct security benefits and involves specific design trade-offs with respect to performance, privacy, and complexity.

Our comparative analysis of blockchain types and consensus mechanisms provides practical guidance for system designers: consortium permissioned blockchains with BFT consensus are generally the most appropriate choice for enterprise IDS deployments, offering the best balance of performance, security, and privacy control. Domain-specific applications in IoT, cloud, and SDN environments each require tailored design decisions that we have examined in detail.

Significant challenges remain—scalability, latency, smart contract security, Sybil resistance, and interoperability—and constitute a rich agenda for future research. Our proposed five-layer reference architecture provides a modular foundation for tackling these challenges and for realising the full potential of blockchain-enhanced IDS in practice. We believe that blockchain represents not a panacea but a powerful and well-motivated addition to the IDS designer's toolkit, and that its responsible integration will meaningfully advance the state of network security.

REFERENCES

[1] Lunt, T. F. (1993). A survey of intrusion detection techniques. Computers & Security, 12(4), 405–418.

[2] Zawoad, S., & Hasan, R. (2013). Digital forensics in the cloud. IEEE Security & Privacy, 11(3), 74–77.

[3] Stiborek, J., Pevny, T., & Rehak, M. (2018). Multiple instance learning for malware classification. Expert Systems with Applications, 93, 346–357.

[4] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Bitcoin.org whitepaper.

[5] Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS). NIST Special Publication 800-94.

[6] Garcia-Teodoro, P., Diaz-Verdejo, J., Macia-Fernandez, G., & Vazquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 28(1–2), 18–28.

[7] Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity, 2(1), 1–22.

[8] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system (Whitepaper). Available at https://bitcoin.org/bitcoin.pdf.

[9] Androulaki, E., Barger, A., Bortnikov, V., et al. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. Proceedings of EuroSys 2018, 1–15.

[10] Golomb, T., Mirsky, Y., & Elovici, Y. (2018). CIoTA: Collaborative IoT anomaly detection via blockchain. Proceedings of NDSS Workshop on Decentralized IoT Security and Standards.

[11] Alexopoulos, N., Vasilomanolakis, E., Le Vinh, N. R., & Muhlhauser, M. (2017). Towards blockchain-based collaborative intrusion detection systems. Proceedings of CRITIS 2017, Lecture Notes in Computer Science, 10707.

[12] Li, W., Tug, S., Meng, W., & Wang, Y. (2019). Designing collaborative blockchained signature-based intrusion detection in IoT environments. Future Generation Computer Systems, 96, 481–489.

[13] Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y., & Han, J. (2018). When intrusion detection meets blockchain technology: A review. IEEE Access, 6, 10179–10188.

[14] Preuveneers, D., Rimmer, V., Tsingenopoulos, I., Spooren, J., Joosen, W., & Ilie-Zudor, E. (2018). Chained anomaly detection models for federated learning: An intrusion detection case study. Applied Sciences, 8(12), 2663.

[15] Pourvahab, M., & Ekbatanifard, G. (2019). Digital forensics architecture for evidence collection and provenance preservation in IaaS cloud environment using SDN and blockchain technology. IEEE Access, 7, 153349–153364.

[16] Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2017). Towards blockchain-based auditable storage and sharing of IoT data. Proceedings of the 2017 Workshop on Cloud-Assisted Networking.

[17] Wuthier, S., Mersy, G., Nwafor, E., & Chang, S.-Y. (2020). Privacy-preserving collaborative intrusion detection through blockchain-managed federated learning. Proceedings of IEEE GLOBECOM 2020.

[18] Rahouti, M., Xiong, K., & Ghani, N. (2018). Bitcoin concepts, threats, and machine-learning security solutions. IEEE Access, 6, 67189–67205.

[19] Liang, G., Weller, S. R., Luo, F., Zhao, J., & Dong, Z. Y. (2019). Distributed blockchain-based data protection framework for modern power systems against cyber attacks. IEEE Transactions on Smart Grid, 10(3), 3162–3173.

[20] Lu, Y., Huang, X., Dai, Y., Maharjan, S., & Zhang, Y. (2020). Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. IEEE Transactions on Industrial Informatics, 16(6), 4177–4186.

[21] Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an optimized blockchain for IoT. Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, 173–178.

[22] Hang, L., & Kim, D. H. (2019). Design and implementation of an integrated IoT blockchain platform for sensing data integrity. Sensors, 19(10), 2228.

[23] Hossain, M., Xu, L., & Hasan, R. (2020). Blockchain-based privacy-aware intrusion detection for smart home environments. Future Generation Computer Systems, 110, 795–804.

[24] Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. Journal of Network and Computer Applications, 36(1), 42–57.

[25] Qin, X., Huang, Y., Yang, Z., & Li, X. (2020). A blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing. Journal of Systems Architecture, 112, 101854.

[26] Kreutz, D., Ramos, F. M. V., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14–76.

[27] Bhatia, S., Khatri, S. K., & Bhatia, A. (2020). Blockchain-integrated SDN for securing smart grid communications. Proceedings of IEEE ICCES 2020.

[28] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352–375.

[29] Ben-Sasson, E., Chiesa, A., Garman, C., et al. (2014). Zerocash: Decentralized anonymous payments from Bitcoin. Proceedings of the 2014 IEEE Symposium on Security and Privacy, 459–474.

[30] Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts (SoK). Proceedings of POST 2017, Lecture Notes in Computer Science, 10204, 164–186.

[31] Douceur, J. R. (2002). The Sybil attack. Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS), 251–260.

[32] Panait, A. E., Olimid, R. F., & Stefanescu, A. (2020). Analysis of uPort open, an identity management blockchain-based solution. Proceedings of CRiSIS 2020, Lecture Notes in Computer Science.