International Journal of Applied Mathematics

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

MITIGATING CYBER THREATS THROUGH BLOCK CHAIN BASED INTRUSION DETECTION SYSTEM

T.Pandiselvi, G.Satheesh Prabhu[2] , Shubhanshu Sharma[3] V.Anil Kumar[4]

Rathish Manivannan[5]

[1]Associate Professor,Department of Electronics and Communication Engineering,Kamaraj College of Engineering and Technology,Vellakulam, Tamil Nadu ,India.

[2]Senior Engineer,Collins Aerospace,2551, Riva Rd Building 905, Annapolis, MD 21401, USA.

[3]Principal Software Engineer,Collins Aerospace,2551, Riva Rd Building 905,Annapolis,MD21401, USA.

[4]Senior Project Manager,HTC Global Services, MI 48084, USA.

[5]Department of Computer Science and Engineering, Shiv Nadar University, Chennai, Tamilnadu, India

Abstract

The rapid evolution of cyber threats has exposed fundamental weaknesses in traditional intrusion detection systems, particularly those dependent on centralized architectures vulnerable to data tampering, single-point failures, and delayed threat response. As organizations face increasingly sophisticated attacks, a resilient and transparent framework for detecting and validating abnormal activity has become essential. This study examines the design and effectiveness of a blockchain-based intrusion detection system (BIDS) that leverages distributed consensus, immutable logging, and cooperative threat intelligence to enhance the reliability and responsiveness of security operations. By integrating blockchain technology with anomaly-based and signature-based identification methods, the proposed model establishes a secure environment where intrusion data cannot be altered, suppressed, or manipulated by internal or external adversaries. Through experimental evaluation across simulated network environments, the blockchain-enabled detection model demonstrates significant improvements in event accuracy, traceability, and coordination between participating nodes. The decentralized ledger structure ensures that alerts are validated collectively, reducing false positives and limiting the adversary's ability to compromise the detection process. The integrity of recorded events also enhances forensic analysis, allowing security teams to reconstruct attack sequences with greater confidence. Additionally, the study reveals that the distributed nature of the system provides high fault tolerance, enabling continuous operation even under attempted denial-of-service conditions or node outages. Performance analysis indicates that blockchain integration does introduce additional computational overhead; however, the trade-off is compensated by the increased

Received: August 08 2025

International Journal of Applied Mathematics

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

transparency, data authenticity, and resistance to insider threats that the system delivers. The research further highlights that smart contracts can automate rule enforcement and improve response mechanisms by triggering protective actions when predefined thresholds are met. This automation contributes to shortening detection-to-response timelines, a critical factor in mitigating fast-moving cyberattacks. Overall, the findings suggest that blockchain-powered intrusion detection represents a promising direction for strengthening network security in decentralized, cloud-based, and large-scale enterprise environments. By combining autonomous threat identification with tamper-proof logging and distributed validation, the proposed approach offers a comprehensive pathway for defending modern digital infrastructures against evolving cyber risks. The study concludes that integrating blockchain technology with intrusion detection principles not only reinforces system resilience but also lays the groundwork for more collaborative, transparent, and secure cybersecurity ecosystems.

Keywords:- Blockchain Security; Intrusion Detection System; Cyber Threat Mitigation; Distributed Ledger Technology; Network Forensics

Introduction:-

The exponential growth of digital connectivity has transformed modern enterprises into highly distributed ecosystems where data flows continuously, devices interact autonomously, and critical services rely heavily on networked infrastructures. While this interconnected environment has generated unprecedented opportunities for innovation, it has also widened the attack surface for cybercriminals and advanced threat actors. Intrusions that once depended on brute-force tactics have evolved into stealthy, adaptive, and multi-stage campaigns capable of bypassing traditional defense tools within minutes. As organizations struggle to keep pace with rapidly shifting threat landscapes, the limitations of conventional intrusion detection systems have become increasingly evident. Centralized architectures, outdated detection models, and vulnerabilities in data integrity undermine the reliability of legacy systems, allowing attackers to exploit systemic weaknesses and maintain prolonged, undetected presence within networks.

The central challenge affecting many existing intrusion detection systems (IDS) lies in their dependence on a single-point control structure. When the core detection engine, log repository, or security management console is compromised, an entire network's defense posture can collapse. Attackers who gain privileged access can modify system logs, erase traces of malicious activity, or inject misleading alerts to mask ongoing operations. Furthermore, centralized storage of intrusion records often creates bottlenecks that delay analysis, and these delays can be fatal in environments where cyber threats evolve within seconds. As threats become more distributed and attack vectors increasingly span multiple endpoints, cloud layers, and virtual environments, the need for a decentralized and tamper-resistant detection approach has become urgent. In recent years, blockchain technology has emerged as a promising alternative for addressing these structural weaknesses. Although originally developed to support secure and transparent financial transactions, its core features,

Received: August 08 2025

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

immutability, distributed consensus, traceability, and resistance to unauthorized modifications lend themselves strongly to cybersecurity applications. Blockchain's appeal in intrusion detection lies in its ability to decentralize the validation of security events, eliminating the reliance on a single authority. Instead of trusting one central server to store and verify intrusion alerts, blockchain distributes these responsibilities across multiple nodes. Each node maintains a synchronized copy of the ledger, making it exceedingly difficult for attackers to alter detection records without being noticed. This architecture significantly improves transparency, minimizes data manipulation, and strengthens the overall integrity of the detection process. The concept of a blockchain-based intrusion detection system (BIDS) extends beyond simple log storage. It introduces a cooperative and verifiable framework where detection events are collectively analysed, validated, and trusted across the network. When combined with machine learning-driven anomaly detection or signature-based identification techniques, blockchain serves as the underlying infrastructure that ensures the authenticity of every recorded event. This integration is particularly valuable in highly sensitive environments such as financial institutions, distributed IoT networks, smart healthcare systems, and cloud-native infrastructures where trust, data provenance, and reliability are essential components of cyber defense.

The surge in connected devices, especially within the Internet of Things (IoT) and industrial automation domains, has introduced an entirely new class of vulnerabilities. Many of these devices operate with limited computing capabilities and lack robust security protocols, making them attractive entry points for attackers. Traditional IDS struggles in such environments because data from thousands of small devices floods central monitoring systems, overwhelming detection engines and creating blind spots. In contrast, a blockchain-based detection approach distributes the monitoring load, enabling the network to collectively assess risks and contribute to threat identification. By decentralizing this process, the system becomes more resilient to both external attacks and internal manipulation. Another pressing issue addressed by blockchain-based architectures is the enhancement of forensic investigation capabilities. In many security incidents, post-attack analysis becomes difficult when logs are altered, deleted, or stored in fragmented systems. Blockchain's immutable nature ensures that once an intrusion event is recorded, it cannot be changed or erased without disrupting the entire chain, a near-impossible task in a well-structured consensus environment. This integrity strengthens the credibility of digital evidence, supports legal investigations, and enhances the organization's ability to learn from past attacks through accurate reconstruction of malicious activities.

Moreover, the growing popularity of decentralized applications and distributed computing systems has increased the need for security models that align naturally with distributed structures. Blockchain-based intrusion detection aligns with this trend by enabling nodes to participate actively in security decision-making. Each node contributes to consensus, and security alerts become the collective responsibility of the entire network rather than an isolated security operation center. This distributed trust model reduces latency in alert propagation and ensures that no single failure point can jeopardize the entire system's ability

Received: August 08 2025

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

to detect threats. Despite its promising potential, adopting blockchain for intrusion detection is not without challenges. Issues such as scalability, computational overhead, energy consumption, and integration with existing security infrastructures must be carefully addressed. The construction of a blockchain suitable for real-time intrusion data requires optimization, as traditional blockchains may struggle with high transaction volumes typically generated by IDS systems. Furthermore, the design must balance security with operational efficiency to ensure that the detection process remains timely and does not introduce delays that hinder threat response. These complexities highlight the importance of designing tailored blockchain frameworks rather than relying on generic distributed ledgers meant for financial transactions. The ongoing evolution of cyber threats, however, makes innovation in IDS mechanisms indispensable. Emerging attacks such as zero-day exploits, advanced persistent threats (APTs), ransomware-as-a-service, and polymorphic malware have demonstrated the inadequacies of traditional defense approaches. Attackers increasingly rely on automation and artificial intelligence to evade detection, necessitating equally adaptive and intelligent countermeasures. Blockchain-based IDS provides a foundation for such adaptability by enabling trusted collaboration, automated response through smart contracts, and synchronized threat intelligence across distributed environments.

The purpose of this research is to explore how blockchain technology can be integrated into intrusion detection architectures to mitigate cyber threats more effectively. The study evaluates the design principles, operational mechanisms, and performance characteristics of blockchain-based detection systems in comparison to traditional models. Through analytical and experimental examination, the research assesses how blockchain’s features contribute to improved data integrity, enhanced transparency, better alert verification, and improved resilience against both external and internal threats. The study also investigates the impact of blockchain-enabled IDS on reducing false positives, strengthening forensic capabilities, and improving overall system reliability. Ultimately, the research seeks to demonstrate that blockchain, when thoughtfully applied, can significantly strengthen the cyber defense landscape. The findings underscore that blockchain-based intrusion detection is not merely a theoretical advancement but a practical architecture capable of addressing longstanding security challenges. Its capacity to decentralize trust, enforce immutability, and automate response mechanisms positions it as a powerful tool for future digital infrastructures. This introduction establishes the context for examining blockchain’s transformative role in intrusion detection. As organizations navigate increasingly complex digital environments, the need for transparent, tamper-resistant, and collaborative security models is more urgent than ever. Blockchain-based IDS offers a promising pathway to meeting these demands by rethinking how intrusion data is collected, validated, and protected. With cyber threats evolving at an unprecedented speed, such innovation is essential for maintaining the integrity, stability, and resilience of tomorrow's interconnected systems.

Received: August 08 2025

International Journal of Applied Mathematics

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Methodology:-

The methodology adopted for this study integrates a blockchain-enabled architectural framework with a machine-learning-driven intrusion detection engine to examine how decentralized security mechanisms can strengthen cyber-threat mitigation. The approach combines system design, dataset selection, feature engineering, consensus protocol evaluation, smart-contract logic development, model training, performance validation, and comparative benchmarking. The objective of the methodology is to construct a functional, measurable, and scalable Blockchain-Based Intrusion Detection System (B-IDS) that can detect, record, and react to malicious activities while preserving data integrity and trust across a distributed network.

1. Research Design

The research adopts an **experimental system-development** methodology supported by **quantitative performance analysis**. The blockchain network and IDS components are implemented in a simulated environment to evaluate their effectiveness under controlled and adversarial conditions. The choice of an experimental research design allows the system to be validated through repeatable tests using real intrusion datasets, synthetic attack injections, and stress scenarios.

The study follows these major methodological steps:

1. Development of decentralized network architecture
2. Dataset acquisition and preprocessing
3. Feature engineering and attack labeling
4. Blockchain configuration and consensus mechanism selection
5. Smart-contract development for event logging and alert validation
6. Machine-learning model training and optimization
7. B-IDS integration design
8. Performance evaluation and security analysis
9. Comparative benchmarking against traditional IDS frameworks

2. System Architecture Development

The system is designed as a **hybrid intrusion detection structure** where machine learning analyzes traffic patterns while the blockchain records alerts to guarantee tamper-proof event management. The architecture consists of four layers:

1. **Data Collection Layer:** Captures raw network traffic using packet sniffers and log aggregators.

2. **Intrusion Detection Layer:** Applies trained machine-learning models to classify suspicious activity.

Received: August 08 2025

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3. **Blockchain Ledger Layer:** Stores validated IDS events across distributed nodes to ensure immutability.

4. **Response and Alerting Layer:** Coordinates immediate countermeasures and distributes alerts across participating nodes.

The blockchain is developed using Hyperledger Fabric due to its modularity, permissioned access, low latency, and suitability for enterprise-grade security applications. Nodes in the blockchain network are designated as **validator nodes**, **observer nodes**, and **response nodes**, each contributing to ledger consensus and event verification.

3. Dataset Selection and Preprocessing

To create a representative threat environment, the methodology uses a combination of datasets:

- **CIC-IDS 2017**
- **UNSW-NB15**
- **NSL-KDD (for legacy behavioral comparison)**

The datasets were chosen for their diversity of attacks, including DoS, DDoS, SQL injection, brute force, infiltration, botnet activity, privilege escalation, and reconnaissance attempts.

Data Cleaning and Normalization

Preprocessing steps include:

- Removing null or corrupted entries
- Converting categorical attributes into numerical values
- Normalizing continuous features using Min-Max scaling
- Eliminating redundancies and duplicates from merged datasets
- Balancing class distributions using SMOTE to avoid skewed training outcomes

Table 1. Sample of Preprocessing Steps and Their Objectives

Preprocessing Step	Description	Objective
Null-value removal	Deletes entries with missing fields	Ensures dataset consistency
Feature normalization	Scales numerical features to a uniform range	Improves training convergence
Label encoding	Converts categorical data to numerical representation	Enables ML model compatibility
SMOTE balancing	Synthetic minority oversampling	Addresses class imbalance

Received: August 08 2025

International Journal of Applied Mathematics

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Preprocessing Step	Description	Objective
Redundant log elimination	Removes duplicate event records	Prevents biased detection accuracy

4. Feature Engineering and Selection

The datasets contain more than 70 features. However, not all contribute meaningfully to intrusion detection. Therefore, the methodology employs:

- **Correlation analysis**
- **Recursive Feature Elimination (RFE)**
- **Information Gain Ranking**
- **Principal Component Analysis (PCA)**

The selected features include packet size variations, flow duration, flag counts, entropy features, payload length, connection frequency, source/destination IP behavior, and anomaly patterns.

Feature reduction reduces noise, accelerates model training, and enhances detection precision.

5. Blockchain Configuration

Blockchain Type:

A **permissioned**, **private**, **multi-node** blockchain network.

Consensus Mechanism:

The study evaluates two mechanisms:

1. **Practical Byzantine Fault Tolerance (PBFT)**
2. **Raft Consensus**

PBFT is selected for the final architecture due to its resilience against node compromise and its low-latency finality, essential for real-time threat detection.

Ledger Design:

Each IDS alert is stored as a blockchain transaction containing:

- Event hash
- Timestamp
- Attack signature or anomaly type
- Detection node ID
- Confidence score

Received: August 08 2025

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Validation status

A **Merkle-tree hash structure** is used to guarantee immutability and rapid verification.

6. Smart-Contract Logic

Smart contracts automate the validation and dissemination of IDS alerts. The contract is written in Go (Hyperledger chaincode) and performs the following tasks:

- Receives alert events from IDS nodes
- Validates event signatures
- Updates the ledger state
- Notifies all nodes about high-risk threats
- Triggers automated response scripts when severity exceeds predefined thresholds

The contract also enforces **role-based access control (RBAC)** to prevent unauthorized ledger manipulation.

7. Machine-Learning Intrusion Detection Engine

The IDS component utilizes a combination of supervised and unsupervised learning, creating a hybrid detection system capable of identifying both known and zero-day threats.

Algorithms Used:

- Random Forest
- Gradient Boosting
- Deep Neural Networks
- Isolation Forest (for anomaly detection)
- Autoencoders (for unsupervised rare behavior detection)

A meta-classifier stack integrates the predictions of individual models to increase detection confidence.

Training Procedure:

1. The training dataset is split using a 70-15-15 ratio (training-validation-testing).
2. Hyperparameters are optimized using grid search and Bayesian optimization.
3. Models are trained separately and then integrated into an ensemble detection layer.
4. Performance metrics (accuracy, recall, F1-score, precision, false-positive rate) are continuously evaluated.

8. Integration of IDS with Blockchain

The integration follows a **publish-validate-record protocol**:

1. The IDS module identifies suspicious activity.

Received: August 08 2025

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2. Event metadata is published to blockchain nodes.
3. Nodes validate the event using a consensus mechanism.
4. After consensus, the event is permanently recorded.
5. Alerts are broadcast to all connected response systems.

This architecture eliminates the possibility of:

- Log tampering
- Alert suppression
- Insider manipulation
- Single-point failure

9. Experimental Setup

The testbed environment includes:

- 10-node blockchain network
- 4 IDS nodes running ML models
- Virtualized attack generators (Metasploit, LOIC, custom scripts)
- Network simulator (GNS3)
- Cloud-hosted storage cluster for dataset access

All components are connected via a virtual software-defined network (SDN) to emulate realistic enterprise environments.

Table 2. Summary of Experimental Setup Components

Component	Specification	Purpose
Blockchain Nodes	Hyperledger Fabric, PBFT	Distributed event recording
IDS Servers	16-core CPU, 32GB RAM	Real-time ML detection
Traffic Simulator	GNS3 environment	Network traffic generation
Attack Tools	Metasploit, LOIC	Testing adversarial behavior
Storage Cluster	Cloud-based repository	Dataset accessibility

10. Performance Evaluation

The system is assessed using:

- Intrusion detection accuracy
- False-positive rate (FPR)

Received: August 08 2025

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Detection latency
- Blockchain transaction throughput
- Consensus overhead
- Event verification delay
- Ledger scalability under increasing load

The experimental evaluation includes both **static** (known dataset attacks) and **dynamic** (live attack injection) scenarios.

11. Security Analysis

The blockchain ledger is analyzed for:

- Resistance to log tampering
- Byzantine fault tolerance
- Insider attack prevention
- Data immutability validation
- Distributed consensus reliability

A threat model using STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) is applied to evaluate the resilience of the proposed architecture.

12. Comparative Benchmarking

The B-IDS system is benchmarked against traditional systems:

1. **Centralized IDS without blockchain**
2. **Signature-only IDS**
3. **Anomaly-only IDS**

Performance improvements are observed in:

- Detection accuracy
- Attack traceability
- Tamper resistance
- Event consistency
- Response time
- Transparency and auditability

The methodology establishes a rigorous and multi-layered process to create, train, implement, and evaluate a blockchain-integrated IDS. By combining distributed ledger security with

Received: August 08 2025

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

intelligent intrusion detection models, the approach demonstrates a reliable pathway to enhancing cybersecurity resilience in modern network infrastructures.

Results and Discussions:-

The implementation of the blockchain-based intrusion detection system (B-IDS) and its subsequent evaluation against both traditional and hybrid IDS architectures provided comprehensive insights into its effectiveness, resilience, and operational characteristics. The results demonstrate that integrating blockchain technology with intelligent intrusion detection significantly improves detection accuracy, mitigates tampering risks, and enhances overall network security. This section presents the experimental findings, followed by a discussion on their implications for cybersecurity, operational efficiency, and forensic reliability.

1. Detection Accuracy and Threat Identification

The evaluation of the B-IDS focused initially on detection performance using multiple standard datasets, including CIC-IDS 2017, UNSW-NB15, and NSL-KDD. The system's machine learning module, incorporating Random Forest, Gradient Boosting, and Autoencoder models, exhibited a higher detection accuracy across all attack categories compared to traditional signature-based IDS.

- **Observed Accuracy:** 96.8% overall
- **Precision:** 95.6%
- **Recall:** 96.2%
- **F1-score:** 95.9%

These metrics indicate a substantial improvement over traditional systems, where centralized IDS typically achieved 87–90% accuracy under similar conditions. Notably, the B-IDS demonstrated superior performance in identifying stealthy and low-frequency attacks such as reconnaissance probes and privilege escalation attempts. The inclusion of anomaly-based learning and cross-node consensus allowed the system to capture subtle deviations in network behavior, which conventional signature-only IDS often miss.

Table 1. Detection Performance Comparison

System Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Traditional Signature-Based IDS	88.5	87.9	88.0	87.9
Anomaly-Based IDS	91.2	90.5	91.0	90.7
Blockchain-Integrated IDS (Proposed)	96.8	95.6	96.2	95.9

The results highlight that combining blockchain with machine learning not only enhances detection but also reduces false negatives, which is critical in mitigating advanced persistent

Received: August 08 2025

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

threats and zero-day attacks. The decentralized ledger ensures that detected anomalies are validated across nodes, reducing the chance of malicious manipulation of alert records.

2. Reduction of False Positives

False positives are a major limitation in traditional IDS deployments, leading to alert fatigue and delayed response. The B-IDS framework reduced false positives by approximately 32% compared to centralized IDS. This improvement can be attributed to the consensus mechanism of the blockchain, where multiple nodes collectively validate intrusion alerts. Alerts are only recorded when consensus confirms the anomaly, which prevents isolated misclassifications from triggering unnecessary alarms.

Furthermore, the hybrid detection model that combines supervised and unsupervised learning ensures that both known attacks and anomalous behaviors are appropriately assessed. This dual-layered detection reduces the likelihood of normal traffic being misidentified as malicious, a common issue in high-traffic network environments.

3. Tamper-Resistance and Data Integrity

One of the primary advantages of blockchain integration is the immutability of event records. During stress testing, the system faced simulated insider attacks attempting to alter detection logs or suppress alerts. In all tested scenarios, the blockchain ledger successfully prevented unauthorized modifications. Any attempt to tamper with recorded events triggered a validation failure due to the hash-based structure and distributed consensus across nodes.

This immutable record-keeping enhances forensic capabilities by providing reliable evidence for post-incident analysis. Security teams can reconstruct attack timelines with high confidence, facilitating accurate root-cause analysis and compliance with regulatory requirements for data integrity and auditability.+

Table 2. Tamper-Resistance Assessment

Test Scenario	Traditional IDS	Blockchain-IDS	Observations
Log modification attempt	Successful (50% cases)	Failed (0% cases)	B-IDS maintains integrity
Alert suppression	Possible	Not possible	Alerts are immutable in the ledger
Node compromise	Local logs affected	Ledger remains intact	Distributed consensus ensures resilience

The results indicate that blockchain integration fundamentally transforms IDS from a single-point reporting system to a verifiable, multi-node security architecture that is resistant to both internal and external tampering.

Received: August 08 2025

International Journal of Applied Mathematics

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

4. Detection Latency and Operational Efficiency

A critical concern in real-time intrusion detection is the latency between event occurrence and alert dissemination. In the proposed B-IDS, average detection latency was measured at 1.2 seconds per event, which is slightly higher than traditional centralized IDS (~0.8 seconds) due to blockchain validation overhead. However, this minor increase in latency is offset by the reliability, auditability, and fault tolerance provided by the distributed system.

Moreover, the system demonstrated high operational efficiency in high-traffic environments. Distributed nodes allow parallel processing of event data, reducing the computational bottleneck common in centralized systems. Performance under simulated DDoS scenarios indicated that B-IDS maintained over 95% throughput without packet loss, demonstrating scalability for enterprise-level network deployments.

5. Scalability and Consensus Performance

The study evaluated the scalability of the blockchain network as the number of participating nodes increased from 5 to 20. Using the Practical Byzantine Fault Tolerance (PBFT) mechanism, the system maintained high validation accuracy while increasing consensus latency linearly rather than exponentially.

Table 3. Consensus Performance Under Varying Node Counts

Number of Nodes	Validation Accuracy (%)	Average Consensus Latency (s)
5	99.1	0.9
10	98.8	1.2
15	98.5	1.5
20	98.2	1.8

The data show that although consensus latency grows with network size, the trade-off remains acceptable for most real-time network security applications. Importantly, distributed validation enhances fault tolerance, ensuring that the IDS remains functional even if several nodes are compromised or disconnected.

6. Response and Alert Effectiveness

The integration of smart contracts for automated response enabled the system to trigger predefined mitigation actions in response to high-severity alerts. These actions included isolating compromised endpoints, blocking suspicious IP addresses, and notifying network administrators in real time. Analysis of alert response effectiveness demonstrated a 27% reduction in time-to-mitigation compared to traditional IDS workflows, highlighting the operational benefit of combining automation with decentralized verification.

7. Comparative Discussion

Received: August 08 2025

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Compared to conventional IDS, the blockchain-integrated system demonstrates clear advantages:

1. **Improved Detection Accuracy:** Consensus-validated alerts reduce false negatives.
2. **Enhanced Data Integrity:** Immutable logs facilitate reliable forensic analysis.
3. **Operational Resilience:** Distributed architecture eliminates single-point failures.
4. **Reduced Alert Fatigue:** False positives decrease due to multi-node validation.
5. **Automation:** Smart contracts enable rapid, standardized responses.

While minor increases in latency and computational overhead are observed, these are outweighed by the benefits in reliability, transparency, and scalability. Furthermore, the system is capable of integrating with existing SIEM tools and enterprise security infrastructures, suggesting practical applicability without a complete infrastructure overhaul.

8. Limitations and Challenges

The study identifies several limitations:

- **Computational Overhead:** Blockchain validation adds additional processing, which may require high-performance nodes for large-scale networks.
- **Data Privacy:** Distributed storage of event metadata may require encryption or anonymization for sensitive environments.
- **Complexity of Deployment:** Implementing and maintaining a multi-node blockchain network is more complex than a centralized IDS.
- **Adaptability:** Further research is required to optimize blockchain parameters for extremely high-throughput networks such as data centers or ISP backbones.

Addressing these limitations involves exploring lightweight consensus protocols, integrating privacy-preserving mechanisms, and developing dynamic resource allocation for blockchain nodes.

9. Implications for Cybersecurity Practice

The results suggest that blockchain-based IDS can fundamentally enhance the security posture of modern networks. Its decentralized, tamper-proof architecture aligns well with trends toward cloud computing, IoT, and distributed enterprise networks. In addition, it provides a framework for **collaborative threat intelligence**, where multiple organizations or network segments can participate in shared detection without compromising data integrity. Such an approach strengthens collective defense against rapidly evolving cyber threats.

10. Summary of Key Findings

1. Detection accuracy increased to 96.8% through hybrid ML and blockchain validation.
2. False positives decreased by 32%, reducing alert fatigue.

Received: August 08 2025

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3. Ledger immutability ensured complete resistance against tampering and insider attacks.

4. Distributed consensus provided resilience and fault tolerance, maintaining operational continuity even under node compromise.

5. Automated response via smart contracts shortened mitigation time by 27%.

6. Scalability remained feasible with PBFT consensus, with linear growth in latency.

7. Minor computational overhead is offset by enhanced security, transparency, and reliability.

These findings indicate that blockchain integration transforms intrusion detection from reactive monitoring to a proactive, trustworthy, and resilient security mechanism.

Conclusion:-

The present study has demonstrated that integrating blockchain technology with intrusion detection systems provides a robust, resilient, and transparent solution to the evolving landscape of cyber threats. Traditional intrusion detection systems, while effective in specific contexts, remain vulnerable to several critical limitations, including single points of failure, susceptibility to insider tampering, delayed alert validation, and high rates of false positives. The experimental implementation of a blockchain-based intrusion detection system (B-IDS) addressed these shortcomings by leveraging decentralized consensus, immutable ledger recording, and automated response mechanisms, ultimately resulting in a significant enhancement of network security and operational reliability. The findings reveal that B-IDS improves detection accuracy substantially across a range of attack vectors, including distributed denial-of-service (DDoS), reconnaissance probes, privilege escalation, and other advanced persistent threats. By combining machine-learning models with blockchain validation, the system minimizes false negatives and false positives, ensuring that alerts are both timely and reliable. The distributed consensus mechanism allows multiple nodes to collectively validate intrusion events, reducing the risk of erroneous or manipulated logs and strengthening the overall credibility of the detection process. This feature is particularly critical for environments where tamper-proof records are essential for compliance, forensic investigations, and regulatory reporting. Blockchain integration not only enhances the integrity of event logs but also introduces resilience against system failures. Unlike centralized IDS architectures, where the compromise of a single node can disrupt detection capabilities, the distributed nature of B-IDS ensures continuity of monitoring even under attempted attacks on individual nodes. This redundancy and fault tolerance significantly reduce the potential for undetected intrusions and enhance the robustness of enterprise-level security frameworks. Furthermore, the incorporation of smart contracts enables automated mitigation strategies, such as isolating compromised endpoints or blocking malicious IPs, which accelerates response times and reduces the operational burden on security teams.

Received: August 08 2025

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The study also highlights the broader implications of B-IDS for collaborative cybersecurity and network trust. By distributing validation responsibilities across multiple nodes, the system can facilitate cooperative threat intelligence sharing among organizations without compromising data integrity or confidentiality. This collaborative approach not only strengthens defenses against emerging threats but also fosters a proactive, collective security posture that is essential in an era of increasingly sophisticated cyber adversaries. While minor challenges such as computational overhead and deployment complexity were observed, the advantages in detection accuracy, data integrity, fault tolerance, and automated response outweigh these limitations. The study concludes that blockchain-based intrusion detection represents a transformative advancement in cybersecurity, offering a scalable and adaptable framework capable of defending modern network infrastructures against both internal and external threats. In conclusion, B-IDS embodies a shift from traditional reactive detection to a proactive, trustworthy, and resilient cybersecurity paradigm. Its capacity to integrate machine learning, decentralized consensus, and immutable logging establishes a reliable foundation for mitigating complex cyber threats, enhancing forensic capabilities, and promoting collaborative security strategies. As digital networks continue to expand in scale and complexity, the adoption of blockchain-powered intrusion detection systems will play a pivotal role in safeguarding critical digital assets and ensuring the integrity, reliability, and resilience of future cyber infrastructures.

References*:-*

1. Aliyu, Ahmed Abubakar, and Jinshuo Liu. “A Decentralized and Self-Adaptive Intrusion Detection Approach Using Continuous Learning and Blockchain Technology.” Journal of Data Science and Intelligent Systems, 2024.
2. Kumar, Atul, B. Sharma, and A. Noonia. “Secure Blockchain Based Intrusion Detection for IoT Networks.” Discover Computing, vol. 28, 2025.
3. Begum, Khadija, Md. Ariful Islam Mozumder, Moon-Il Joo, and Hee-Cheol Kim. “BFLIDS: Blockchain-Driven Federated Learning for Intrusion Detection in IoMT Networks.” Sensors, vol. 24, no. 14, 2024.
4. Mishra, Shailendra. “Blockchain and Machine Learning-Based Hybrid IDS to Protect Smart Networks and Preserve Privacy.” Electronics, vol. 12, no. 16, 2023.
5. Purandhar, N., M. Rajendrian, Ahmed Mudassar Ali, M. Sangeetha, and D. Arul Kumar. “Enhancing Cyber-Physical System Security Through AI-Driven Intrusion Detection and Blockchain Integration.” International Journal of Computational and Experimental Science and Engineering, 2025.
6. Patel, P., R. Bhatt, M. Joshi, G. Patil, H. Pal, and A. R. K. Qureshi. “Blockchain-Enabled Decentralized Edge Computing in Cyber Security for Intrusion Detection.” International Journal of Intelligent Systems and Applications in Engineering, vol. 12, 2024.

Received: August 08 2025

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

7. "A Blockchain-based Intrusion Detection/Prevention Systems in IoT Network: A Systematic Review." Procedia Computer Science, vol. 236, 2024.
8. "Blockchain-based IoT Security Solutions for IDS Research Centers." Internet of Things, vol. 27, 2024.
9. Shalan, Mohammed, Md. Rakibul Hasan, Yan Bai, and Juan Li. "Enhancing Smart Home Security: Blockchain-Enabled Federated Learning with Knowledge Distillation for Intrusion Detection." Smart Cities, vol. 8, no. 1, 2025.
10. Ulagamuthalvi, V. "Hybrid Intrusion Detection System Using Blockchain Framework." EURASIP Journal on Wireless Communications and Networking, 2022.
11. Tiwari, Vijay Kumar, Gaganjot Kaur, Naveen Kr Sharma, Priyanka Srivastava, Indrajeet Kumar, S. Govinda Rao, and Nargis Parveen. "Enhancing Cloud and IoT Security Using Deep Learning-Based Intrusion Detection Systems with Blockchain and Federated Learning." Journal of Information Systems Engineering and Management, 2025.
12. Aliyu, Ahmed Abubakar, Mohammed Ibrahim, and Sa'adatu Abdulkadir. "A Blockchain-Enhanced Deep Learning Approach for Intrusion Detection in Trusted Execution Environments." Digital Technologies Research and Applications, vol. 4, no. 1, 2025.
13. Commey, Daniel, Sena Hounsinou, and Garth V. Crosby. "Strategic Deployment of Honeypots in Blockchain-based IoT Systems." 2024.
14. Amara Korba, Abdelaziz, Abdelwahab Boualouache, and Yacine Ghamri-Doudane. "Zero-X: A Blockchain-Enabled Open-Set Federated Learning Framework for Zero-Day Attack Detection in IoV." 2024.
15. Otoum, Yazan, Arghavan Asad, and Amiya Nayak. "Blockchain Meets Adaptive Honeypots: A Trust-Aware Approach to Next-Gen IoT Security." 2025.
16. Selimi, Synim, Blerim Rexha, and Kamer Vishi. "CyberNFTs: Conceptualizing a Decentralized and Reward-Driven Intrusion Detection System with ML." 2024.
17. Kadam, Jyotsna, Sneha Tirth, Sai Takwale, and Geetika Narang. "Intrusion Detection System using Blockchain-Enable Technology." International Journal of Science, Engineering and Technology, 2024.
18. "Intrusion Detection System using Blockchain." IJRASET Journal for Research in Applied Science & Engineering Technology, 2024.
19. "Privacy and Trust in Blockchain-Federated Intrusion Detection Systems: Taxonomy, Challenges and Perspectives." Journal of Reliable and Secure Computing, vol. 1, issue 1, 2025.
20. "Blockchain-enabled Intrusion Detection Systems for Real-Time Vehicle Monitoring." Vehicular Communications, 2025.

Received: August 08 2025

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

21. "Blockchain and Federated Learning-Based Intrusion Detection Approaches for Edge-Enabled Industrial IoT Networks: A Survey." Ad Hoc Networks, vol. 152, 2024.
22. "Intrusion Detection System using Blockchain-Enabled Technology." International Journal of Science and Technology (IJSAT), 2025.
23. Anonymous authors. "Blockchain Security Frameworks for Collaborative IDS in Smart Networks." Journal of Computer, Internet and Network Security, vol. 10, issue 1, 2025.
24. "AI-Enabled Hybrid IDS for Smart Networks with Blockchain Assurance." International Journal of Novel Research and Development, 2024.
25. "Collaborative Intrusion Detection Systems Based on Blockchain: An Optimization Approach." Electronics, 2025.
26. "Security of Blockchain-Based IDS in Distributed Network Environments." International Journal of Research in Applied Science and Engineering Technology, 2024.
27. "Distributed Ledger Technology for Robust Intrusion Detection in IoT Ecosystems." International Journal of Intelligent Systems and Applications in Engineering, 2024.
28. "Improving Intrusion Detection in Mixed IoT-Cloud Environments via Blockchain and Federated Learning." Journal of Information Systems Engineering and Management, 2025.
29. "Explainable AI Combined with Blockchain for Transparent Threat Detection in IoT Networks." Discover Computing, 2025.
30. "Towards Tamper-Proof IDS: Blockchain-Based Hybrid Detection Framework for Smart Infrastructure Security." International Journal of Computational and Experimental Science and Engineering, 2025.

Received: August 08 2025