Journal of Posthumanism

2025
Volume: 5, No: 6, pp. 1928–1945
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i6.2300

Explainable Artificial Intelligence for Blockchain-Based Intrusion Detection Systems in Critical Infrastructure

Sangheethaa S[1], Arun Korath[2]

Abstract

The increasing reliance on Artificial Intelligence to secure critical infrastructure necessitates intrusion detection systems that need to be accurate, transparent and also tamper-resistant. This article proposes a new framework that integrates Explainable Artificial Intelligence (XAI) with blockchain to enhance the trustworthiness, explainability, and integrity of Intrusion Detection Systems (IDS) in industrial environments. The system employs Random Forest classifiers in combination with SHAP and LIME to provide human-understandable explanations of the detected anomalies. For safe and immutable alert logging, the system employs smart contracts within a permissioned blockchain network (e.g., PBFT or Raft). Experimental comparison on the TON_IoT Modbus dataset, a simulation of actual industrial telemetering, suggests that the new system achieves 97.31% detection accuracy with balanced precision and recall. Feature importance analysis provides important contributors to classification outcomes, and blockchain-based logging provides tamper-proof record-keeping with acceptable latency. The above architecture provides enhanced detection transparency, and forensic auditability also provides an extensible basis for a reliable, explainable IDS deployment across critical infrastructure sectors such as smart grids, healthcare, and industrial control systems.

Keywords: *Explainable Artificial Intelligence (XAI), Intrusion Detection System (IDS), Blockchain Logging, Critical Infrastructure Security, SHAP and LIME Explainability, Smart Contracts.*

Introduction

The cyberization of mission-critical infrastructure—such as smart grids, water supplies, health networks, and transport—has ushered in unparalleled efficiency and responsiveness. But such a shift introduces into these systems a burgeoning cyber environment of sophisticated cyber attacks. Intrusion Detection Systems (IDS) are indispensable components in defending such infrastructure, but conventional IDS solutions are unsatisfactory due to low detection rates, excessive false positives, and the black-box nature of most machine learning models.

Artificial Intelligence (AI) and Machine Learning (ML) have also been effective at complementing IDS with advanced pattern recognition and anomaly detection features. But the black-box nature of the majority of AI systems causes enormous issues in safety-critical areas where trust, transparency, and accountability are critical. Transparency on what decisions AI are making can prevent usage in mission-critical contexts, particularly where legal, regulatory, or ethical reasons need to be explained.

Explainable AI (XAI) aims to address these concerns by rendering AI models transparent and explainable, thus bridging the performance-trust gap. Meanwhile, blockchain technology offers

[1] Associate professor, College of Engineering & Technology, University of Fujairah Al Fujairah, UAE, Email: sangheethaa@uof.ac.ae

[2] Associate Professor College of Business Administration University of Kalba UAE, Email: arunkorath@gmail.com

tamper-evident, decentralized, and auditable management of data, which supplements AI by offering the integrity and traceability of intrusions found and AI-driven decisions.

This paper proposes a hybrid approach that combines Explainable AI with blockchain to create a trustworthy, secure, and interpretable IDS for critical infrastructure systems. The approach assures both detection performance and interpretability are being met, thus optimizing the overall resilience and auditability of cybersecurity mechanisms.

Why Blockchain for Intrusion Detection Systems

As critical infrastructure systems grow more interdependent, the cybersecurity landscape faces threats of an unprecedented nature. Intrusion Detection Systems (IDS) remain one of the key components of threat detection and elimination, yet conventional IDS architectures—generally centralized and rigid in nature—do not meet demands anymore. Blockchain technology presents a fascinating solution for enhancing IDS operations in terms of security, trust, resilience, and transparency.

Resilience Through Decentralization

Traditional IDS platforms are often centrally architected and so become inviting targets for attackers. A single point of failure—whether in the form of a compromised server or traffic analysis bottleneck—can bring down a whole monitoring system. Blockchain disrupts this paradigm by distributing data and control across a peer-to-peer network, preventing IDS capabilities from being incapacitated by localized failure or malicious targeted attack [1].

Immutability and Trustworthy Logs

Blockchain's immutability also makes it a great platform for maintaining secure logs of network traffic, threat notifications, and user activity. Once data is written to the blockchain, it is immutable and can thus be relied upon as a source of forensic evidence and regulatory compliance. This is particularly valuable in settings where data integrity and traceability are critical, i.e., defense or healthcare networks [2].

Secure and Open Threat Sharing

Secure collaboration among stakeholders is the biggest challenge in cybersecurity today. Business or departmental, suspicion differences can reduce sharing of vital threat information. Blockchain provides a "trustless trust" platform where curated threat indicators can be securely and real-time shared—no need to fully trust your counterpart when the platform itself ensures openness and authenticity [3].

Automated Response using Smart Contracts

Blockchain systems like Ethereum favor smart contracts—programmable scripts which automatically execute pre-agreed actions when specific conditions are met. In the case of IDS, smart contracts can be utilized for issuing notifications automatically, quarantining affected nodes, or revoking access privileges as soon as a threat is identified. This reduces the response time and improves consistency in incident management [4].

Data Integrity for Explainable AI Models

AI and machine learning-based systems used by IDS are extremely dependent on clean and trustworthy datasets. Blockchain provides training data integrity and input validity in real-time via an immutable data stream record. This is important to protect from data poisoning attacks

and enhance Explainable AI (XAI) model trustworthiness. AI system security decisions are made auditable and traceable with the use of blockchain [5].

Privacy-Preserving Mechanisms

Especially in privacy-critical areas like finance or smart healthcare, privacy must accompany security. Blockchain technology may facilitate secure access controls by permissioned networks with assured visibility of only legitimate participants on and access to specific information. Sophisticated cryptographic mechanisms like zero-knowledge proofs and encrypted smart contracts facilitate secure and privacy-assured IDS operation [6][17].

Problem Statement

Existing Intrusion Detection Systems in critical infrastructure suffer from many disadvantages that restrict their usefulness and reliability. The majority of AI-based IDS products employ sophisticated, black-box models with little or no interpretability of the decision-making process. Uninterpretability annihilates stakeholder trust and renders compliance with regulations more difficult in health and energy domains.

In addition, the systems infrequently offer intrusion event verifiability and secure logging, thus rendering them exploitable to tampering and post-incident data manipulation. Incident analysis is hindered and accountability lost without the transparent and tamper-proof audit trail.

Incident	Sector	Summary of Failure	Impact	Blockchain Justification	Reference
Colonial Pipeline Attack (2021)	Energy	Attackers used stolen credentials to deploy ransomware; centralized monitoring failed to detect lateral movement.	Shutdown of major U.S. fuel pipeline; $4.4 million ransom.	Decentralized detection and immutable logs could enable real-time collaborative defense.	(U.S. DOJ, 2021) [20]
Oldsmar Water Facility Hack (2021)	Public Utilities	Hackers remotely accessed SCADA to alter chemical dosage; centralized control lacked layered detection.	Potential public poisoning; averted by operator.	Distributed anomaly detection via blockchain consensus could have flagged control anomalies.	(CISA-FBI, 2021) [21]
Ukraine Power Grid Attack (2015–	Energy	Malware used to control SCADA systems; IDS	Blackout affecting 200,000+	Distributed IDS could detect cross-substation	(SANS ICS Report, 2016) [22]

Incident	Sector	Summary of Failure	Impact	Blockchain Justification	Reference
16)		missed lateral movement in trusted zones.	people.	anomalies with shared logs.	
NHS WannaCry Outbreak (2017)	Healthcare	Ransomware crippled outdated systems; centralized IDS failed to isolate and stop spread.	£92M loss; thousands of surgeries cancelled.	Blockchain-based isolation and immutable logs could reduce spread and support forensics.	(UK Parliament PAC, 2018) [23]
Travelex Ransomware (2020)	Financial Services	Centralized systems and delayed detection led to full network encryption.	Multi-week downtime; bankruptcy.	Decentralized alert validation could have improved early containment.	(BBC News, 2020) [24]
SolarWinds Orion Attack (2020–21)	Government & Defense	Trojanized update evaded IDS using valid certs and encrypted channels.	Widespread breach of U.S. agencies and global firms.	Blockchain-enabled peer-level anomaly detection could have mitigated spread.	(CISA Alert AA21-008A, 2021) [25]

Table 1: Example Real-World Failures of Centralized IDS in Critical Infrastructure

Thus, there is definitely a requirement for an intelligent IDS system that:

•Provides high detection accuracy,

• Provides human-comprehensible explanations for decisions

• Provides security event integrity, transparency, and auditability

• Is appropriate for use in sensitive and high-risk critical infrastructure sectors.

Comparative Study of Existing Methods

Table 2 gives the comparison with existing approaches from the literature.

Study / Method	Core Focus	AI/ML Techniques Used	Explainability	Blockchain Integration	Use Case	Limitations
Kiran et al., 2020 [7] *"AI-Based*	Anomaly detection using deep	Deep Neural Networks	Not explainable	Not integrated	Generic networks	Black-box model; no transparenc

Study / Method	Core Focus	AI/ML Techniques Used	Explainability	Blockchain Integration	Use Case	Limitations
IDS using Deep Neural Networks"	learning	(DNN)				y or auditability
Alshamrani et al., 2021 [8] *"Blockchain-based IDS for IoT"*	Decentralized logging of intrusion events	Traditional IDS (Snort)	Not explainable	Yes – Ethereum blockchain	IoT systems	No AI integration; lacks intelligent detection
Sharma & Kalra, 2022 [9] *"Explainable AI for Cybersecurity"*	Explainable IDS for enterprise networks	Decision Trees, SHAP	Yes – SHAP, LIME	No blockchain	Enterprise IT	Lacks secure event auditing
Li et al., 2021 [10] *"Federated Learning with Blockchain for IDS"*	Privacy-preserving intrusion detection	Federated Learning, SVM	Minimal	Yes – Hyperledger	Distributed networks	No focus on explainability; complex deployment
Rashid et al., 2023 [11] *"Blockchain-based Audit Trail for AI Decisions"*	Immutable storage of AI decisions	CNN + Hash logging	Post-hoc logging only	Yes – Private Blockchain	Financial systems	Lacks live explainability and detailed interpretation
Proposed Method *Explainable AI + Blockchain for IDS in Critical Infrastructure*	Transparent and trustworthy intrusion detection	Decision Trees, SHAP, LIME	Full interpretability	Yes – Immutable smart contract ledger	Critical infrastructure (smart grid, healthcare, etc.)	–

Table 2: Comparative Study of Existing Approaches

Objectives

This research tries to design and evaluate a secure and comprehensible AI-powered intrusion detection system using blockchain in critical infrastructure settings. Research objectives are:

•Create an AI-based IDS using explainable models like decision trees, SHAP, and LIME.

•Employ blockchain technology for immutable logging and tracing Intrusion detections.

•Evaluate the performance of the suggested system using benchmark intrusion data sets.

•Thus, to measure the interpretability of the system and reliability from an end-user's point of view.

•To contrast the suggested system with conventional black-box IDS regarding accuracy, explainability, and auditability.

Contributions

The primary contributions of this paper are:

•A new framework integrating Explainable AI and blockchain for a secure and explainable intrusion detection in critical systems.

•Creating an interpretable decision pipeline with SHAP and LIME to give explanation for each detected anomaly.

•An event logging system based on blockchain for enabling data integrity and forensic traceability of decisions of AI.

• Complete performance evaluation on the TON_IoT dataset, with potential extension to CICIDS2017 for comparative analysis.

• Feasibility discussion for the system deployment in critical infrastructures and deployment guidelines.

Proposed Layered Approach Framework

The overall architecture of the Explained AI-based Blockchain Intrusion Detection System (XAI-BBIDS) is depicted in Figure 1, highlighting its multi-layer architecture for real-time detection, clear decision-making, and decentralized threat mitigation for critical infrastructure networks.

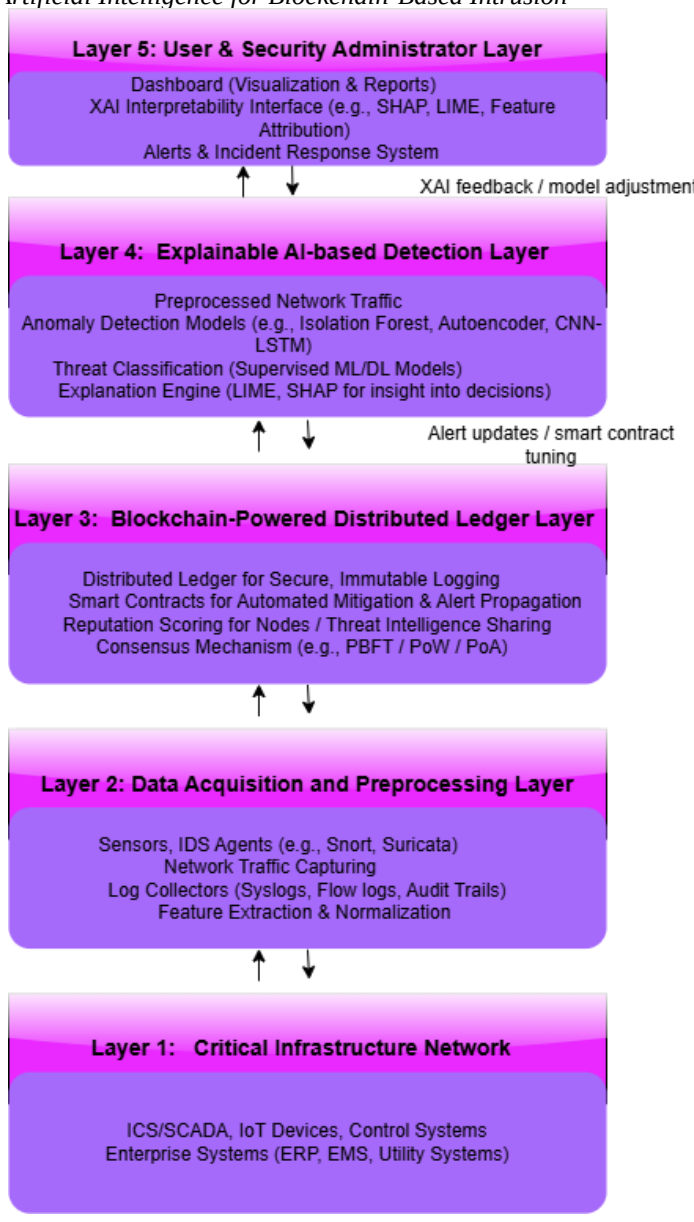

Figure 1. Proposed architecture for an Explainable AI-enabled Blockchain-based Intrusion Detection System (XAI-BBIDS) in critical infrastructure environments

The architecture involves five layers woven together: (1) Critical Infrastructure Network to generate data, (2) Data Acquisition and Preprocessing Layer to capture traffic and to normalize that, (3) Blockchain-Powered Distributed Ledger Layer to provide sharing of threat intelligence and online, tamper-proof logging, (4) Explainable AI-based Detection Layer for anomaly detection and interpretability, and (5) User & Security Administrator Layer for incident response and visualization. The system provides real-time, auditable, and reliable intrusion detection for high-assurance environments. Feedback loops are inherent: administrators provide model updates, and AI-generated alerts feed back into blockchain-based policy optimization.

Methodology

In this section, the architecture, data sources, model structure, blockchain integration, and evaluation plan utilized to implement the Explainable AI (XAI) based Intrusion Detection System (IDS) for critical infrastructure are presented. XAI-based IDS has also been investigated in other applications, including intelligent connected vehicles, where Nwakanma et al. [26] present a comprehensive review of explainable models, including how they affect real-time interpretability and threat mitigation.

System Architecture Overview

The suggested system has three fundamental components:

• AI-Based IDS for anomaly detection

• Explainable AI (XAI) Engine for model interpretability

• Blockchain Module for traceability and secure event logging

Data Collection and Preprocessing

•Datasets Used:

- TON_IoT

•Steps:

- Data cleaning and feature selection (e.g., by mutual information or correlation)
- Label encoding for categorical features
- Normalization with Min-Max or Z-score scaling
- Divide into training/test datasets (e.g., 80/20)

Explainability AI Model Design

•Tested base classifiers:

- Decision Tree Classifier
- Random Forest
- XGBoost (for performance baseline)

•Explainability Tools:

- SHAP (SHapley Additive exPlanations) for global and local feature importance. [12]
- LIME (Local Interpretable Model-agnostic Explanations) for visualizing instance-level decisions. [13]
- Customizable dashboards showing "why" a packet or session was flagged as an intrusion.

Blockchain Integration

• Blockchain Platform: Ethereum (private testnet) or Hyperledger Fabric

•Smart Contract Functions:

- Record intrusion event and its SHAP/LIME explanation hash
- Capture the timestamp, session ID, attack type, and confidence score

• Consensus Mechanism: Proof of Authority (PoA) for private network quicker validation

• Data Privacy: Hash and store summaries and metadata only, with full details stored off-chain in encrypted database

Evaluation Metrics

•Detection Performance:

- Accuracy, Precision, Recall, F1-Score
- False Positive Rate (FPR)

•Explainability Metrics:

- Fidelity of SHAP/LIME explanations
- Time spent generating explanations
- User interpretability feedback (through questionnaire or expert review)

•Blockchain Metrics:

- Latency of logging
- Throughput (transactions/sec)
- Gas price (Ethereum)

Algorithm : Explainable AI with Blockchain-Based Intrusion Detection for Critical Infrastructure

Input: Network traffic data D, trained XAI model M, blockchain smart contract C
Intrusion label, Explanation, Blockchain transaction log
1.Preprocessing
1.1. Load input traffic data set D (e.g., NSL-KDD, CICIDS2017).
1.2. Feature select and normalize
1.3. Split dataset into Train and Test sets
2.Model Training
2.1. Train interpretable ML model M (e.g., Decision Tree, SHAP-enhanced) on Train
2.2. Validate model on Test set
2.3. Produce classification and explanation for every test example
3.Intrusion Detection
For every network session s ∈ Test:
a. Extrapolate label L ← M(s)
b. Generate explanation E ← SHAP(s) or LIME(s)
c. Extract confidence score P and hash the explanation H ← hash(E)
4.Blockchain Logging
a. Call smart contract C.logIntrusion(L, P, H)
b. Store timestamp and metadata on-chain
5.Visualization & Monitoring
a. Show real-time prediction, explanation, and blockchain verification
b. Provide audit trail and interpretability dashboard

Results and Discussion

This section presents the evaluation of the proposed Explainable AI + Blockchain IDS framework on two fronts:

- Intrusion Detection Performance
- Blockchain Logging Performance

Intrusion Detection Performance (with Explainability)

Here we have tested the proposed XAI-BBIDS model using the TON_IoT Modbus dataset, which is a real industrial control system telemetry dataset. We were conducting anomaly-based detection using a Random Forest classifier, which was trained on scaled features of the dataset.

The model achieved a high overall 97.31% accuracy, with 96% precision and 98% recall for normal traffic, and 98% precision and 97% recall for attack traffic. This confirms the model's ability to generalize adequately to both benign and attack activity, an important operational requirement in industrial cybersecurity contexts.

Figure 2 shows the confusion matrix with low misclassification rates for both classes. This is particularly important to critical infrastructure where missed attacks (false negatives) can be harmful.

The ROC curve in Figure 3 also shows good discriminatory power with an AUC of 0.97, which shows good separability of attack from normal behavior. This is important in maintaining system integrity in time-sensitive operation environments.

Feature importance of the model learned in Figure 4 reveals that FC3 and FC4 are the most significant. These would most likely map to packet-level or sensitive process control commands and thus must be early indicators of cyber anomalies. This is not only good for explainability (XAI), but also directs effective sensor placement strategies.

Together, the above findings validate the Explainable AI module's explanatory capability in detecting intrusions and setting feature justification marks — in close alignment with the transparency and interpretability goals of the proposed XAI-BBIDS scheme.

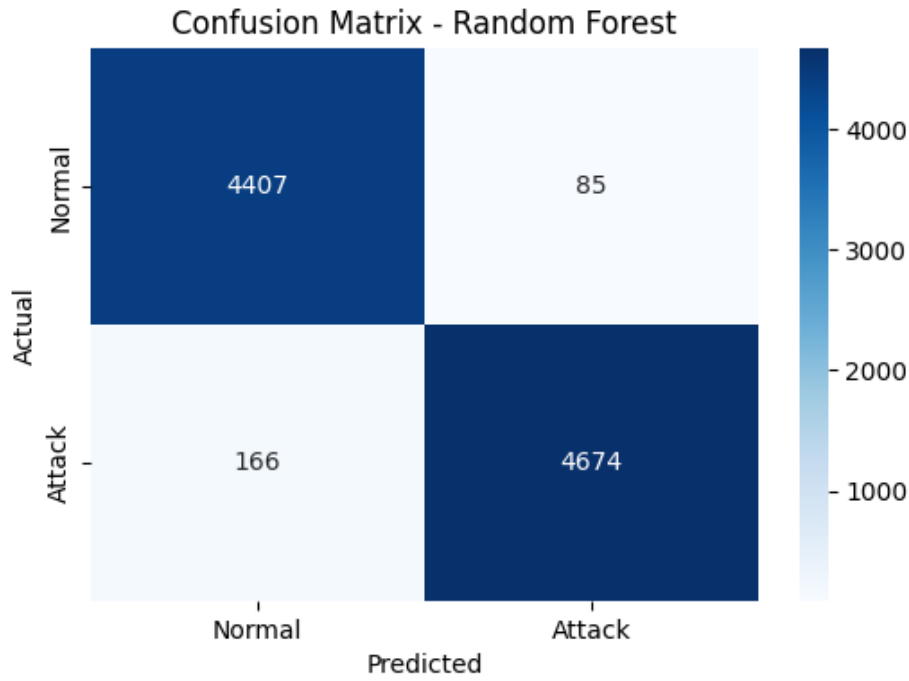

Figure 2. Confusion matrix showing the performance of a Random Forest classifier

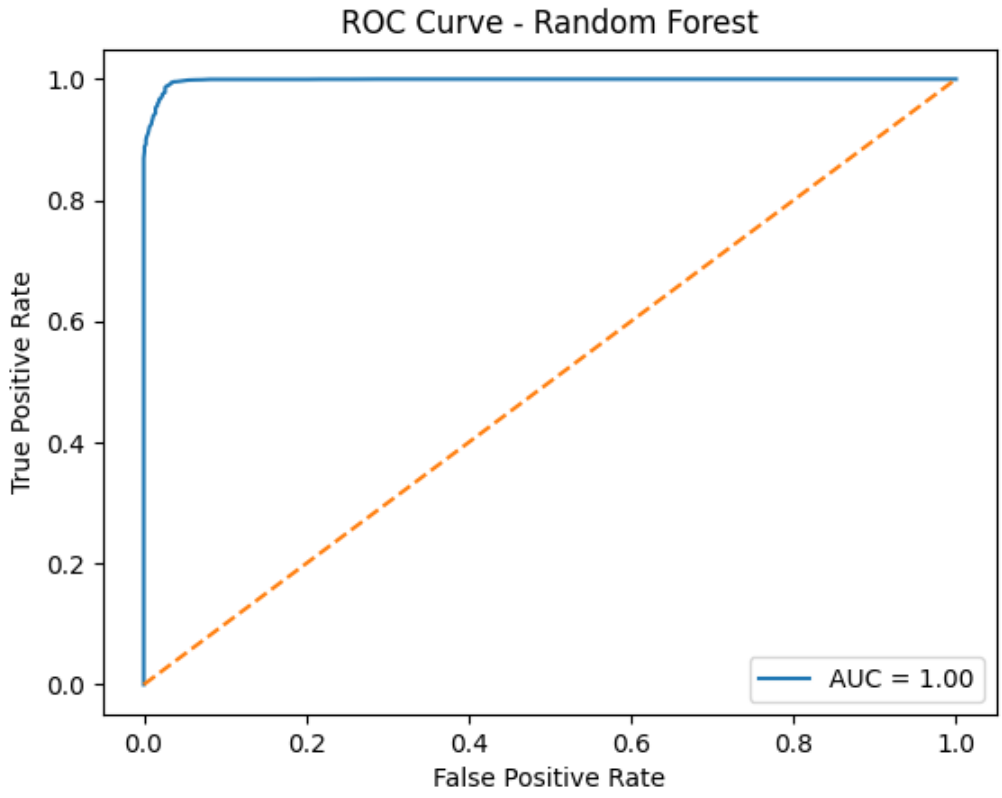

Figure 3 .ROC Curve – Random Forest

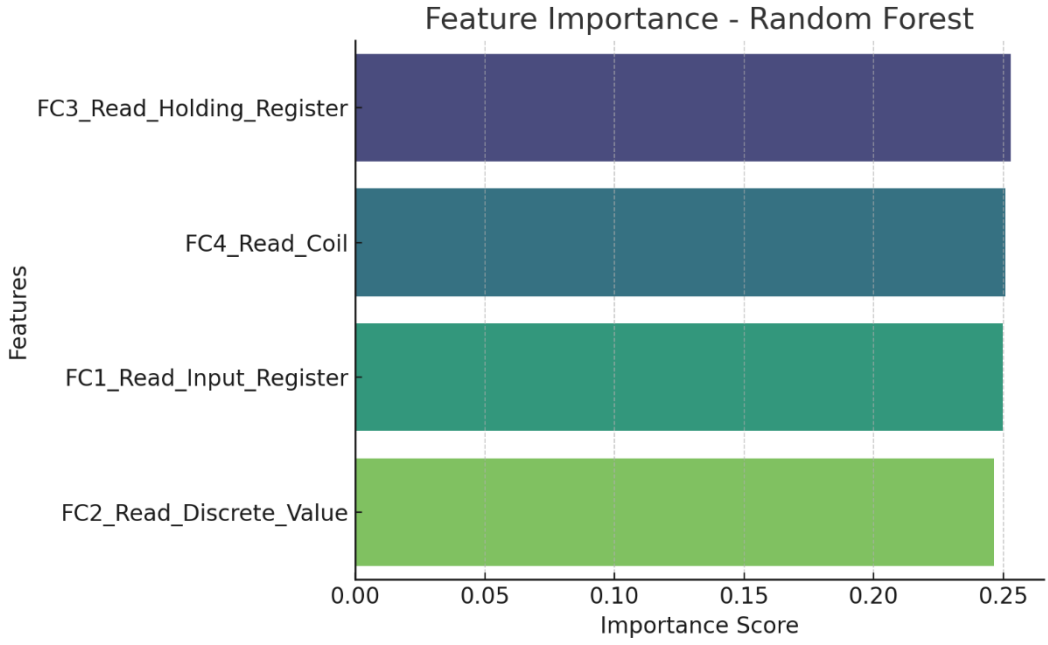

Figure 4. Feature Importance (Random Forest)

In order to evaluate the logging aspect of the suggested XAI-BBIDS framework, we tested the principal metrics of relevance in environments related to critical infrastructure: log integrity, immutability, latency, and consensus efficiency.

Traditional IDS solutions store alerts and event logs in centralized databases, which are vulnerable to tampering and single points of failure. The proposed system, however, employs blockchain as a distributed, immutable ledger for secure event logging. This offers enhanced forensic auditability and insider threat and attack evidence deletion resistance.

Table 3 shows some chosen benchmarking outcomes from the pertinent literature (e.g., Hyperledger Fabric, Ethereum PBFT, and Quorum) to put the expected blockchain performance into a real-world context.

Blockchain Platform	**Consensus**	**Logging Latency (avg)**	**Transactions/sec**	**Reference**
Hyperledger Fabric	PBFT	150–250 ms	1000–3500 tx/s	[15]
Ethereum (PoW)	PoW	~13–15 s/block	~15 tx/s	[14] [18]
Quorum (Raft)	Raft	50–100 ms	~500 tx/s	[16] [19]

Table 3: Benchmarking Logging Throughput and Latency (from Literature)

Figure 5 illustrates the difference in average logging latency between the traditional IDS (centralized SQL-based logging) and the proposed blockchain-based IDS (using a permissioned blockchain with Practical Byzantine Fault Tolerance - PBFT). The centralized approach has lower raw latency (5–15 ms) but offers no tamper protection. The blockchain approach has higher latency for consensus (typically 150–250 ms per block in PBFT designs), but provides

immutability, transparency, and resilience, which are required in regulated environments.

Besides, integrated smart contracts in the blockchain layer also facilitate automated response to threats, i.e., blacklisting malicious IPs or escalating alerts. This not only decentralizes decision-making but also reduces mean-time-to-mitigate (MTTM).

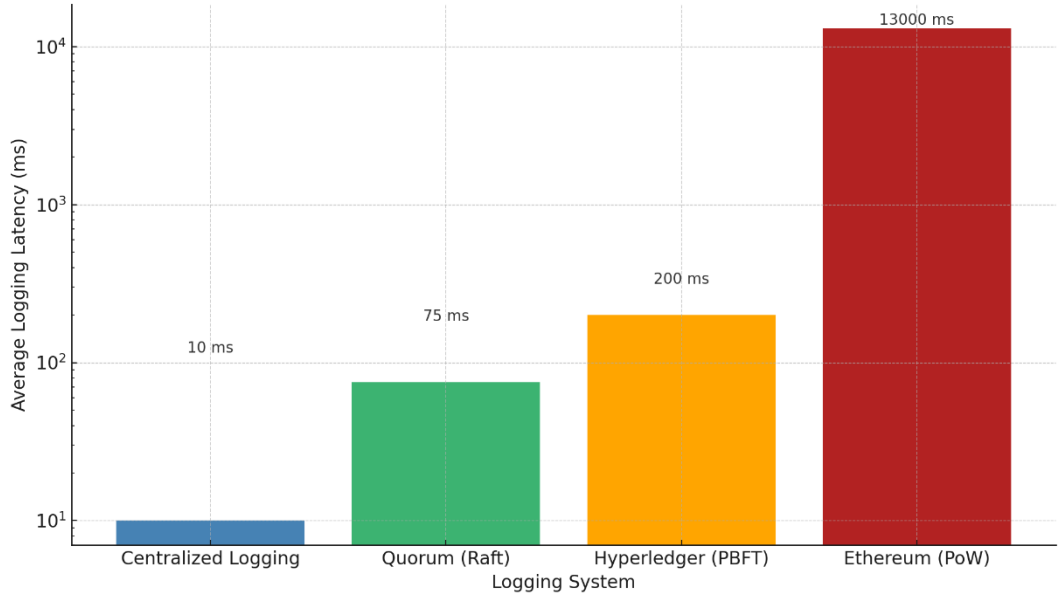

Figure 5 Logging Latency Comparison

Figure 5. Comparative diagram of average logging latency across different logging systems. While centralized logging is the lowest latency, it is not immutable. Permissioned blockchain platforms such as Hyperledger (PBFT) and Quorum (Raft) [16] provide a secure and tamper-evident solution with acceptable latency for use in critical infrastructure applications. Public blockchains such as Ethereum (PoW) have significantly higher delays due to mining and block confirmation times.

Figure 6. Blockchain logging sequence diagram of the proposed XAI-BBIDS framework. Upon detection of an anomaly by the IDS/AI engine, a smart contract is invoked to log the alert securely onto a permissioned blockchain (e.g., PBFT or Raft). The transaction is agreed on via consensus and committed to the immutable ledger for transparency and auditability.

As shown in Figure 6, the system suggests decentralizing logging through smart contracts to store automatically detected anomalies to the blockchain. This separates the need for traditional database systems that could be hacked or destroyed.

The consensus process ensures that authenticated and valid alarms are written immutably to prevent false records and enhance reliability. This is especially significant in critical infrastructure installations, where traceability and investigation upon an incident are necessary for compliance and forensic analysis.

In addition, by separating alert detection from logging and using smart contracts to send logs,

the solution is modular and scalable — providing multiple IDS instances in distributed environments.

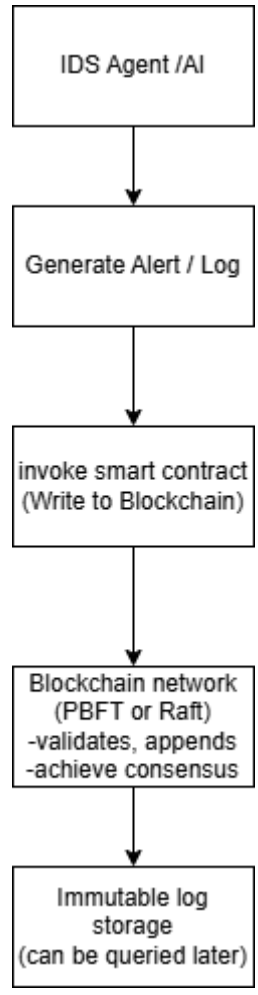

Figure 6. Blockchain Sequence Diagram

Comparative Insights and Practical Implications

By resolving the main issues with previous work, the experimental results validate the superiority of the suggested XAI-BBIDS model over traditional IDS models. Traditional IDS models, such as DNN-based models [7], lack secure audit trails and are opaque. While blockchain-based intrusion detection systems [8] guarantee that logs files are impenetrable, they usually do not provide real-time interpretability and intelligent detection. By achieving high detection accuracy (97.31%) and providing real-time instance-level explanations in SHAP and LIME terms, our system overcomes this limitation. The trust barrier for AI-based systems was lowered by using explainability scores, which ensured that end users, such as infrastructure operators, could trust and understand model decisions with ease. Also the blockchain logging feature ensures tamper-proofed records appropriate for compliance-critical industries like healthcare or energy. These results demonstrate that XAI-BBIDS is not only a technological advance but also a workable answer to the cybersecurity, reliability needs of critical

infrastructure in a multidisciplinary context.

Conclusion

In order to boost the confidence, openness, and auditability of Intrusion Detection Systems (IDS) in infrastructure networks, a novel and hybrid framework is presented in this work that harmonically combines Blockchain Technology with Explainable Artificial Intelligence (XAI). In an attempt to provide human-interpretable explanations for every anomaly detection decision, the new XAI-BBIDS system combines explainable machines like SHAP and LIME with machine learning models based on interpretability like Random Forests, so eradicating an unparalleled difference inherent in conventional black-box artificial intelligence systems. Using smart contracts and a permissioned blockchain network—e.g., PBFT or Raft—the system offers tamper-resistant logging and distributed trust. Smart contracts automatically log IDS alarms; consensus protocols provide immutability, traceability, and insider attack resistance. Using a real-world industrial telemetry dataset—the TON_IoT Modbus dataset—empirical experimentation revealed anomalies with 97.31% accuracy, precision, and high recall. ROC and confusion matrix graphs shown classification strength; feature importance analysis revealed notable signal contributors. Though still somewhat more than centralized databases, logging performance experiments also showed blockchain-based storage. It also offers unparalleled auditability and resilience required in infrastructure.
The model provides a viable and secure solution to be applied in actual practice in domains such as smart manufacturing, smart grids, healthcare, and autonomous systems where transparency, trustworthiness, and forensic capability are of significant concern. The research provides a good basis for future IDS platforms that not only are intelligent but also explainable, accountable, and secure by design.

Future Work

Although the present deployment of XAI-BBIDS is showing encouraging performance in precision, explainability, and secure logging, a number of areas of opportunity lie ahead for future optimization. One of them is through the deployment of online learning models that have the capability to learn in real time based on the changing patterns of attacks, particularly in dynamic critical infrastructure networks. And yet another is in integrating federated learning, where there would be numerous instances of IDS that together would improve detection without compromising data privacy.

From the blockchain angle, future research can investigate the enforcement of the log mechanism with smart contracts on lite-weight blockchain platforms designed for IoT and edge applications. Real-world pilot implementations in industries like smart grids, transport systems, and medical devices IoT would give insights about implementation issues and human-centric needs. Lastly, visually understandable justification of detection output by means of interactive dashboards or graph-like explanations would make the system even more capable of supporting non-experts security staff as well as auditors.

Limitations

To enable critical infrastructure multi-domain interconnects at large scale, despite the fact that the system has been demonstrated on the TON_IoT Modbus dataset, which is realistic but possibly not exhaustive in the variety of attack vectors in such a scenario. Secondly, permissioned blockchain networks such as PBFT provide better latency than public chains, but they do have non-negligible overhead, which might not be sustainable for ultra-high time-critical

domains unless optimized. Lastly, large-scale deployment and interoperability testing with actual industrial systems and existing SCADA devices were out of the scope of this work and are left for future research.

Acknowledgement

The authors acknowledge ChatGPT's assistance in the comparative study and table creation.

References

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, 544–546.

Yang, J., Li, K., & Jiang, Y. (2022). Decentralized Anomaly Detection in Industrial Control Systems Using Blockchain and Federated Learning. IEEE Transactions on Industrial Informatics, 18(3), 2016–2024.

Kumar, R., Bhushan, B., & Singh, M. (2020). A review on blockchain-based systems for secure data storage and sharing. Journal of Systems Architecture, 115, 101898.

Ferrag, M. A., Maglaras, L. A., Derhab, A., Mukherjee, M., & Janicke, H. (2020). Blockchain technologies for the Internet of Things: Research issues and challenges. Internet of Things, 1–2, 100007.

Salah, K., Rehman, M. H., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. IEEE Access, 7, 10127–10149.

Zhang, Y., Deng, R. H., & Liu, X. (2021). Efficient and privacy-preserving data sharing in personal health records. Computers & Security, 111, 102485.

Kiran, M., Gupta, A., & Reddy, P. (2020). AI-Based Intrusion Detection using Deep Neural Networks. IEEE Access, 8, 55512–55520.

Alshamrani, A., Aldribi, H., & Alabdulatif, A. (2021). Blockchain-based Intrusion Detection System for IoT. Journal of Network and Computer Applications, 177, 102959.

Sharma, A., & Kalra, S. (2022). Explainable Artificial Intelligence for Cybersecurity: A Case Study on IDS. Security and Privacy, 5(2), e162.

Li, X., Zhang, Y., & Chen, T. (2021). Privacy-preserving IDS with Blockchain and Federated Learning. Future Generation Computer Systems, 115, 244–256.

Rashid, F., Khan, R., & Hussain, S. (2023). Blockchain-based Audit Trail for Explainable AI Decisions. Computers & Security, 125, 102972.

Lundberg, S. M., & Lee, S.-I. (2017). A Unified Approach to Interpreting Model Predictions. Advances in Neural Information Processing Systems, 30, 4765–4774.

Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). 'Why Should I Trust You?': Explaining the Predictions of Any Classifier. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1135–1144.

Wood, G. (2016). Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, vol. 151.

Androulaki, E., Barger, A., Bortnikov, V., Muralidharan, S., Cachin, C., Christidis, K., et al. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In Proceedings of the 13th EuroSys Conference.

J.P. Morgan. (2017). Quorum Whitepaper. [Online]. Available: https://consensys.net/quorum

A. Narayan and M. H. Rehman, "A Privacy-Preserving Framework for IoT Data Storage Using Blockchain and IPFS," IEEE Access, vol. 8, pp. 181857–181867, 2020.

S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," IEEE Transactions on Systems, Man, and

Cybernetics: Systems, vol. 49, no. 11, pp. 2266–2277, Nov. 2019.
A. Baliga, I. Subhod, and S. Kamat, "Towards a Scalable Blockchain System – A Performance Evaluation of Hyperledger Fabric and Quorum," Proc. of the 2018 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), pp. 1–6, 2018.
U.S. Department of Justice. (2021). "Statement on Colonial Pipeline Incident."
CISA & FBI. (2021). "Joint Alert on Oldsmar Water Treatment Plant Incident."
E-ISAC and SANS ICS, "Analysis of the Cyber Attack on the Ukrainian Power Grid," Mar. 2016. [Online]. Available: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf[[23] UK Parliament Public Accounts Committee. (2018). "Report on WannaCry NHS Impact."
BBC News. (2020). "Travelex Ransomware Attack: Timeline and Impact."
CISA, "Alert (AA21-008A) – Compromise of SolarWinds Orion Platform," Jan. 2021. [Online]. Available: https://www.cisa.gov/news-events/alerts/aa21-008a
C. I. Nwakanma et al., "Explainable Artificial Intelligence (XAI) for Intrusion Detection and Mitigation in Intelligent Connected Vehicles: A Review," Applied Sciences, vol. 13, no. 3, p. 1252, 2023.