Integrating XAI and Blockchain to Enhance Security and Resilience in Industrial Operations

Love Allen Chijioke Ahakonye[1], Hamza Ibrahim[2], Cosmas Ifeanyi Nwakanma[3], Jae Min Lee[2], Dong-Seong Kim[2] *

[1] ICT Convergence Research Center, *Kumoh National Institute of Technology*, Gumi, South Korea

[2] IT-Convergence Engineering, *Kumoh National Institute of Technology*, Gumi, South Korea

[3] Lane Department of Computer Science and Electrical Engineering, *West Virginia University*, Morgantown, United States

* NSLab Co. Ltd., *Kumoh National Institute of Technology*, Gumi, South Korea

cosmas.nwakanma@mail.wvu.edu, (loveahakonye, hamza, jimpaul, dskim)@kumoh.ac.kr

***Abstract*—Industrial systems are increasingly exposed to cyber–physical threats as sensing, automation, and machine learning (ML)-driven control expand the operational attack surface. This work introduces an integrated XAI–Blockchain framework that combines an interpretable one-dimensional convolutional neural network (1D-CNN) and long short-term memory (LSTM) intrusion detection models with PureChain's tamper-resistant logging to secure end-to-end industrial data flows. Experimental results demonstrate that the system achieves real-time detection with low-latency explanation generation, maintaining a high explanation stability of 0.98. It supports reliable access control by blocking 100% of unauthorized attempts and provides deterministic, near-linear blockchain logging suitable for industrial Internet of Things (IIoT) operations. The framework improves security transparency, operational continuity, and auditability, demonstrating its practical viability for resilient industrial environments despite the limitations, notably elevated false-positive rates and low tamper-detection performance. These are key areas for enhancement. Future work will refine the ML models and explanation mechanisms to reduce misclassification, improve interpretability fidelity, and strengthen security through enhanced authentication and encryption.**

***Index Terms*—Blockchain, Cybersecurity, Explainable AI, Industrial IoT, Intrusion Detection, PureChain, PoA^2, XAI**

I. Introduction

Industrial systems are undergoing rapid transformation as advanced sensing, automation, and data-driven control reshape modern production environments [1]. Growing interconnectivity has expanded cyber–physical attack surfaces beyond the capacity of traditional security frameworks to manage effectively [2]. Recent incidents in manufacturing, energy, and process industries demonstrate how adversarial actions, anomalous behaviors, and opaque decision pipelines can cascade through operational technology (OT) networks, causing substantial downtime and safety risks [3]. Integrating Machine learning (ML) into industrial control compromises deterministic guarantees, magnifies sensitivity to data drift and adversarial inputs, and puts strict real-time budgets under pressure. Coupled with limited interpretability and legacy integration barriers, these factors collectively elevate safety and security risks [4]. Although data-driven models enhance efficiency and predictive maintenance, their limited interpretability undermines operator trust and complicates validation under adversarial or uncertain conditions [5].

Explainable Artificial Intelligence (XAI) provides interpretable, human-aligned insights for complex industrial models through attribution techniques, surrogate explanations, and causal reasoning [6]. While these methods improve transparency and support informed oversight, they do not inherently ensure the integrity, provenance, or tamper resistance of operational data or model outputs. In high-stakes industrial environments, explanations must also be verifiable, auditable, and immutable to sustain trust in autonomous decision-making [7].

Blockchain technologies offer decentralized consensus, immutability, and cryptographic integrity, enabling secure and trustworthy data sharing across heterogeneous industrial systems without centralized control [8], [9]. These properties make blockchain well-suited for environments that demand operational integrity, traceability, and resilience against malicious manipulation. However, blockchains alone lack semantic understanding of data flows and cannot provide interpretability or insight into the decision-making processes of advanced analytics components.

Integrating XAI with blockchain offers a fused approach to improving industrial security, transparency, and operational resilience [10]. The combination of interpretable machine intelligence and tamper-proof data governance enables accurate, explainable anomaly detection, and the secure recording, verification, and traceability of events and decisions. This integration supports emerging Industry 5.0 requirements for trustworthy autonomy, decentralized coordination, and human-AI collaboration. Motivated by escalating cyber-physical threats and increasing reliance on AI analytics, this research presents an integrated XAI-blockchain framework that combines interpretable ML models with blockchain's immutable logging capabilities to address interpretability and security in industrial control systems.

This study makes the following contributions:

1) Development and validation of an integrated XAI-blockchain framework that secures industrial control systems by providing real-time anomaly detection alongside transparent, tamper-proof event logging.
2) Evaluation of the performance of 1-dimensional convolutional neural network (1D-CNN) and long short-term memory (LSTM) models for intrusion detection in

industrial scenarios, assessing their accuracy and latency while analyzing interpretability through SHAP-based explanations.
3) Assessment of a custom blockchain (PureChain) integration in providing immutable logging and verifiable audit trails for industrial cybersecurity.
4) Investigation of trade-offs between system performance and explainability in industrial cybersecurity, specifically addressing challenges such as false positive rates, tamper detection, and explainability fidelity.

II. Related Work

A. AI and XAI in Industrial Cybersecurity

Traditional AI models can detect sophisticated IIoT cyber threats but generally function as opaque "black boxes," limiting operator trust and auditability, an issue especially problematic in critical infrastructure [11]. Prior efforts, such as Zolanvari et al. [12] model-agnostic TRUST XAI framework and other XAI-driven approaches, improve interpretability by generating human-readable explanations for threat detection. However, these studies focus on explanation mechanisms rather than ensuring the integrity, authenticity, and tamper resistance of both the explanations and the underlying security data.

B. Blockchain for Data Integrity and Security

Blockchain has been widely investigated for its decentralized, immutable, and transparent storage, which supports trust and data integrity in domains such as supply chains and smart grids [8]. In cybersecurity, prior work shows that blockchain can preserve traceability and provenance of data and AI model activity, for example, by storing model metadata in a permissioned ledger to create tamper-proof forensic audit trails [13]. However, these approaches focus solely on secure logging and lack the interpretive capabilities of XAI needed to explain the reasoning behind recorded events.

C. Integrated AI and Blockchain Approaches

Recent research increasingly combines AI with blockchain to provide end-to-end secure and transparent solutions [8], [13], [14]. One study introduces a blockchain-assisted federated learning framework for IIoT digital twins, leveraging explainable AI to improve interpretability while ensuring tamper-resistant data management [15]. Another integrates XAI with blockchain to strengthen the trust and integrity of industrial intrusion detection systems (IDS) by applying local explanation methods of the Shapley Additive Explanations (SHAP) and Local Interpretable Model-Agnostic Explanations (LIME) and recording alerts through smart contracts, illustrating the practical viability of embedding explainability and auditability into critical security functions [16].

D. Summary of Findings

The current research on XAI-blockchain integration in industrial systems is primarily conceptual, with limited implementation in real-world environments. Existing models, though advancing intrusion detection, lack a unified, validated framework combining XAI for interpreting system behavior and blockchain for securing industrial data flows. This work addresses that gap by proposing a comprehensive XAI-blockchain framework for enhancing security and operational resilience at an industrial scale. Our approach integrates 1D-CNN and LSTM models with SHAP explanations for accurate intrusion detection and interpretability. The 1D-CNN detects short-term anomalies in IIoT traffic, while the LSTM captures long-term dependencies, improving attack pattern detection. SHAP provides transparency by attributing feature contributions to model predictions. Security events are logged on the PureChain blockchain for immutability and auditability, ensuring traceable and accountable decisions in high-stakes industrial settings.

III. System Model

The experimental framework in Fig. 1 adopts a multi-layered architecture designed to evaluate security, resilience, and operational performance across the IIoT environment. The system integrates AI-based intrusion detection with the PureChain blockchain using the PoA^2 consensus mechanism. This ensures synchronized detection, logging, and response, enabling the study to analyze how model predictions, SHAP explanations, and blockchain operations interact within a unified pipeline. The architecture addresses three core objectives: (i) accurate and timely threat detection, (ii) verifiable and tamper-proof auditability, and (iii) deterministic mitigation through a structured control policy. The integration of ML, PureChain, and the response engine establishes a coherent end-to-end workflow that preserves trust, reduces latency, and maintains operational continuity in industrial environments.

A. Integration of AI Models and PureChain Blockchain

The study integrates two 1D-CNNs and an LSTM into the PureChain blockchain through a continuous feedback pipeline. The system facilitates real-time threat detection, transparent logging, and structured performance evaluation across window sizes of 1, 5, and 10. The integration operates under the following steps:

- **Real-time Event Generation**: Each model processes IIoT traffic samples and outputs predictions with a confidence score.
- **SHAP Explanation Mapping**: Each prediction is immediately interpreted using SHAP, producing contribution scores that describe the significance of each feature.
- **PureChain Logging**: Model outputs and explanation metadata are serialized and transmitted to the PureChain network.
- **PoA^2 Validator Verification**: Trusted validators authenticate, sign, and finalize each event through authority and reputation-based association.
- **Event Finalization and Auditing**: Upon consensus approval, the event becomes an immutable ledger entry, forming the basis for resilience analysis and performance tracking.

This tightly coupled workflow ensures that detection, explanation, and logging occur in a synchronized sequence rather than in a delayed or decoupled manner.

B. ML-Based Intrusion Detection Layer

Modeling the data as a multivariate time series, the mapping process begins with feature reduction and normalization to ensure the dataset is suitable for input to the 1D-CNN and LSTM networks. Let the raw IIoT traffic be represented as $D = \{d_1, d_2, \ldots, d_t\}, \quad d_i \in \mathbb{R}^m$. A preprocessing function Φ extracts normalized temporal windows as $X_t = \Phi(d_{t-k}, \ldots, d_t), \quad X_t \in \mathbb{R}^n$. Each model M_θ computes class probabilities over $C = \{c_{normal}, c_{attack_1}, \ldots, c_{attack_p}\}$, expressed in Equation 1.

$$M_\theta(X_t) = P(c \mid X_t) = \left(p_t^{(c_{normal})}, \ldots, p_t^{(c_{attack_p})}\right)^T. \quad (1)$$

After preprocessing, the dataset is split at a 70%/30% ratio to train 1D-CNN and LSTM models to classify samples into normal or attack categories. Each prediction is accompanied by real-time SHAP values that quantify feature contributions, thereby enhancing model interpretability. The final prediction is $y_t = \arg\max_{c \in C} P(c \mid X_t)$. The models' outputs and SHAP explanations are logged on the PureChain blockchain, ensuring immutability and auditability. This integrated pipeline of data processing, model predictions, explanation generation, and blockchain logging guarantees reproducibility and verifiability at each step.

C. PureChain PoA^2 Logging Process

PureChain receives model outputs and explanation results as security events. Each event is validated using PoA^2, which combines validator authority and reputation. The PureChain ledger, as an immutable state machine, stores each finalized event as $E_k = \{\tau, H(E_{k-1}), y_t, p_t, metadata, \sigma_{V_i}\}$. The validator selection probability is based on Equation 2.

$$P(V_i) = \frac{\mathrm{Rep}(V_i)}{\sum_{j=1}^{m} \mathrm{Rep}(V_j)}, \quad (2)$$

where $\mathrm{Rep}(V_i)$ denotes the reputation value assigned to validator V_i, and the denominator represents the cumulative reputation of all m validators. A higher reputation score increases selection probability, ensuring that trustworthy and consistent validators play a more influential role in consensus formation. Logging latency is computed as $L_{log} = \tau_{finality} - \tau_{creation}$. The deterministic response layer activates system actions using a confidence-based policy defined as $a_t = \Delta(S_t, (y_t, p_t), \Pi)$, where the selected action depends on the model prediction and its corresponding explanation confidence. The control logic is formalized as in Equation 3.

$$a_t = \begin{cases} \text{quarantine}, & y_t = c_{malicious} \wedge p_t \geq \tau_{high} \\ \text{throttle}, & y_t = c_{suspicious} \wedge \tau_{low} \leq p_t < \tau_{high} \\ \text{allow}, & \text{otherwise} \end{cases} \quad (3)$$

where y_t is the predicted class label at time t, p_t is the explanation confidence score, and τ_{high} and τ_{low} are predefined confidence thresholds. The classes $c_{malicious}$ and $c_{suspicious}$ correspond to critical and moderate threat levels, respectively. This policy ensures that high-confidence malicious events trigger immediate isolation (*quarantine*), medium-confidence threats invoke rate limiting (*throttle*), and low-risk or uncertain events are permitted (*allow*). End-to-end latency is $L_{E2E} = t_{response} - t_{occurrence}$. The system dynamics evolve as $S_{t+1} = G(S_t, a_t, E_k)$, while the blockchain ledger $B = (E_1, E_2, \ldots, E_k)$ forms a permanent audit trail used for resilience evaluation.

IV. Experimental Setup and Case Studies

A. System Implementation

The experimental setup was implemented in Python 3.10, with initial development on Google Colab and final deployment on a Windows 11 workstation with an Intel Core i5-12400F processor, 32 GB RAM, and an NVIDIA GeForce RTX 3050 GPU. This configuration supported concurrent machine learning and blockchain operations. The blockchain was simulated with seven validator nodes and a quorum of five for consensus, as is typical for medium-scale IIoT systems. The PureChain SDK was integrated with web3.py and a custom wrapper to encrypt and encode client data into blocks. Experiments used public benchmark datasets in a simulated environment, rather than a physical IIoT testbed.

B. Dataset Description

The proposed framework was evaluated using the IoT-CAD dataset [17], a large-scale IoT forensics resource designed for cyberattack detection and attribution. The dataset includes over 530,000 samples from Windows (61 features) and Linux (76 features), covering system, process, and network activity. It spans seven attack classes and fourteen subtypes, with each sample labeled to support fine-grained attribution (What, How, Why). IoT-CAD promotes deep learning, explainable AI, and federated IDS research and underwent preprocessing, including feature reduction, normalization, and redundancy removal, to improve model efficiency.

C. SHAP Case Studies

Fig. 2 presents the SHAP summary plot, which reveals that network-intensive features—particularly `Ethernet0_bytes_sent`, `disk_read_time_percent`, `swap_memory_percent_used`, and `virtual_memory_percent_used`—exert the most decisive influence on the model's predictions. High feature values (red) consistently push outputs toward higher anomaly likelihoods, while CPU-related metrics and differential network-byte changes contribute moderately with bidirectional effects. Collectively, these patterns indicate that the model predominantly relies on memory pressure and network throughput characteristics to distinguish between normal and anomalous IIoT system states.

Fig. 3 presents the SHAP bar plot, which shows that `Ethernet0_bytes_sent` overwhelmingly dominates

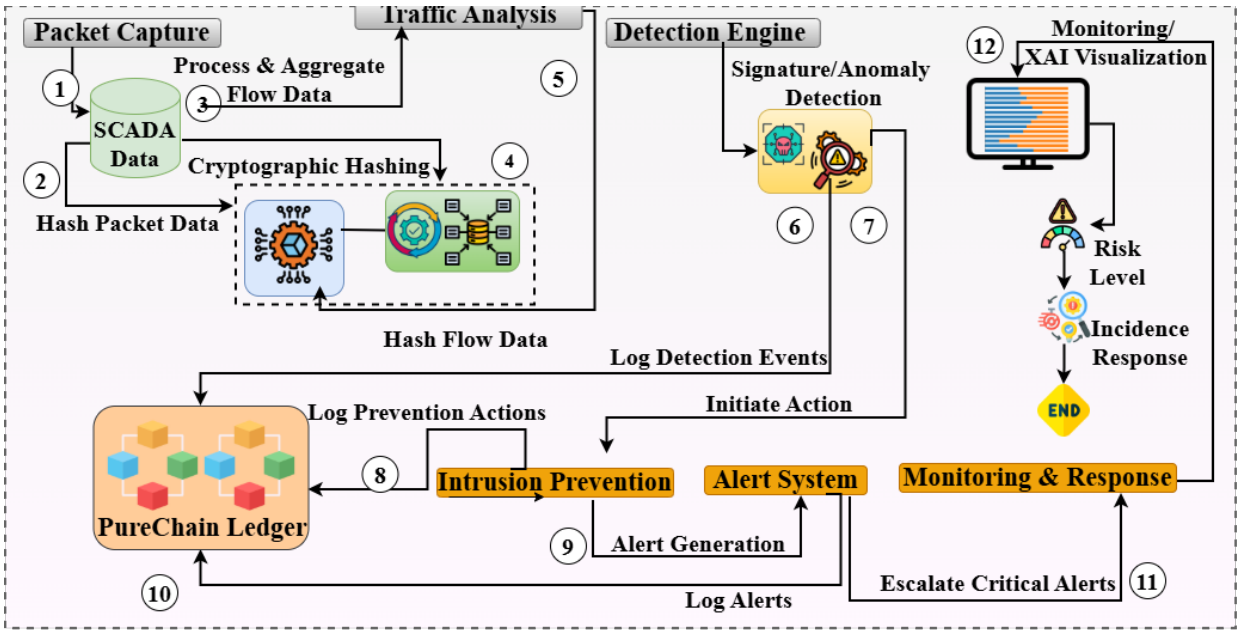

Fig. 1. Design details of the proposed PureChain-based IDPS architecture illustrating the interaction of the involved entities.

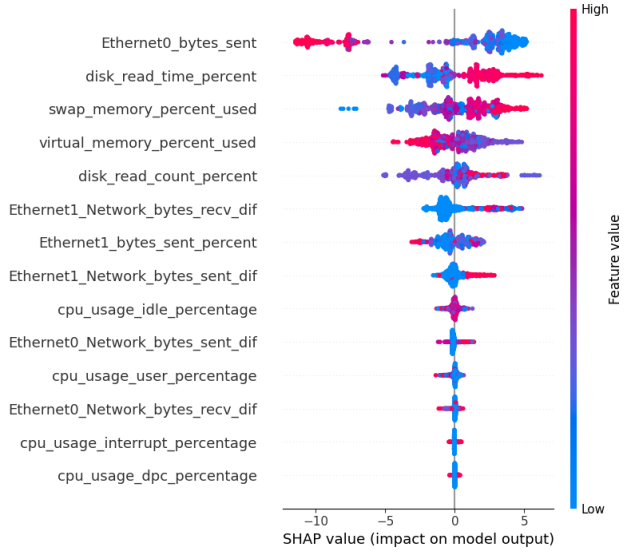

Fig. 2. SHAP summary plot showing feature contributions for intrusion detection.

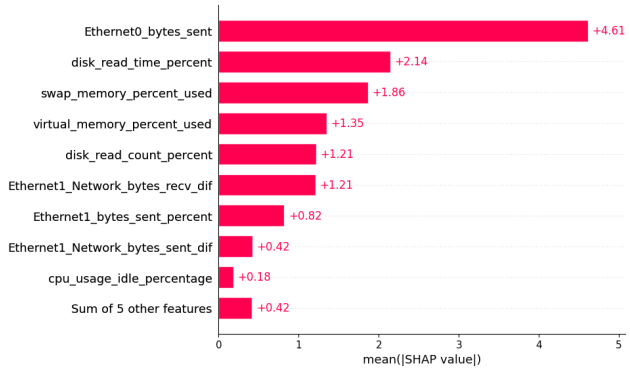

Fig. 3. SHAP feature importance bar plot for the intrusion detection model.

feature importance (mean $|\text{SHAP}| \approx 4.61$), followed by substantial contributions from `disk_read_time_percent`, `swap_memory_percent_used`, `virtual_memory_percent_used`, and `disk_read_count_percent`. Secondary network metrics such as `Ethernet1_Network_bytes_recv_dif` and `Ethernet1_bytes_sent_percent`, along with CPU idle percentages, exhibit comparatively minor influence. Overall, this indicates that the model primarily relies on network throughput and patterns of memory/disk activity to differentiate anomalous from normal IIoT behavior.

Fig. 4 presents the normalized mean absolute SHAP analysis, which reveals that network-traffic differentials—particularly `Ethernet1_Network_bytes_recv_dif` and `Ethernet1_Network_bytes_sent_dif`—are the most influential predictors across both classes. For Class 1, the model relies more heavily on anomalous send/receive patterns, indicative of potential data exfiltration or command-and-control behavior. In contrast, Class 0 is more strongly influenced by system-level metrics such as `cpu_usage_idle_percentage`, `virtual_memory_percent_used`, and `disk_read_time_percent`. These results demonstrate that effective IDS design requires integrating high-granularity network telemetry with host-resource indicators to capture class-specific attack signatures and enhance detection robustness.

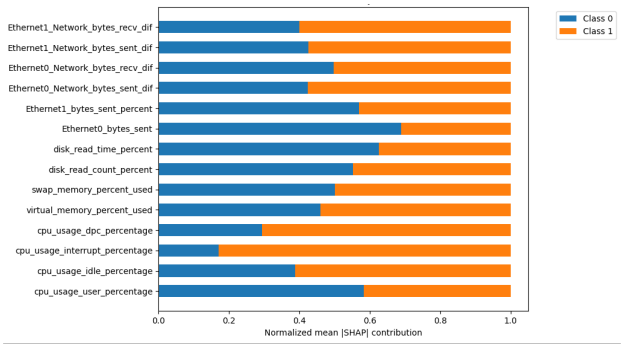

Fig. 4. Normalized mean absolute SHAP values for Class 0 and Class 1.

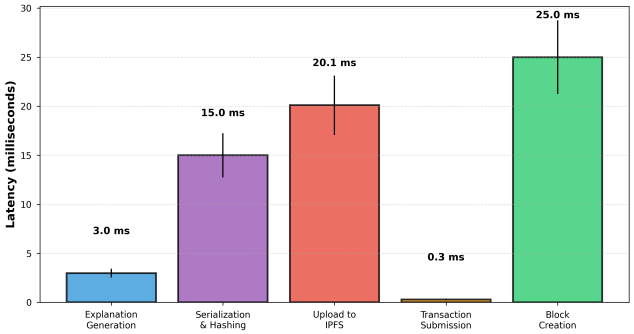

Fig. 6. End-to-end latency breakdown for blockchain logging stages.

Fig. 5 shows that `cpu_usage_user_percentage` exhibits a nonlinear, threshold-like influence on the model's predictions, increasing sharply within the 20–60% range before reaching saturation. This effect becomes substantially more pronounced when `virtual_memory_percent_used` is simultaneously high, revealing a strong interaction between CPU load and memory pressure. These results suggest that concurrent stress on both computational and memory resources provides a more reliable indicator of anomalous IIoT behavior than either metric considered independently.

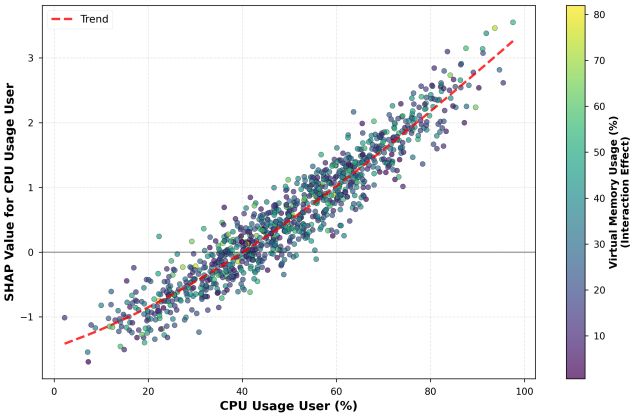

Fig. 5. SHAP dependence plot for `cpu_usage_user_percentage` vs. `virtual_memory_percent_used`.

D. Blockchain Case Studies

Fig. 6 depicts latency analysis, revealing heterogeneous delays across processing stages: explanation generation incurs minimal overhead ($\sim$ 3 ms), serialization & hashing introduces moderate cryptographic delay ($\sim$ 15 ms), IPFS uploading contributes significant network-dependent latency ($\sim$ 20 ms), transaction submission remains nearly instantaneous ($\sim$ 0.3 ms), and block creation produces the highest consensus-related delay ($\sim$ 25 ms). Collectively, these results show that end-to-end latency remains within acceptable limits for secure, near-real-time IIoT operations.

Fig. 7 presents the blockchain growth timeline, showing a stable linear increase in block height with uniformly spaced blocks. This indicates deterministic PoA^2 consensus, where blocks are created every $\sim$ 3–4 seconds, which is significantly faster than on public chains. The absence of forks or reordering confirms an uncongested, reliable environment, demonstrating that the proposed blockchain configuration supports predictable, efficient, and real-time-compatible logging, which is essential for IIoT security operations.

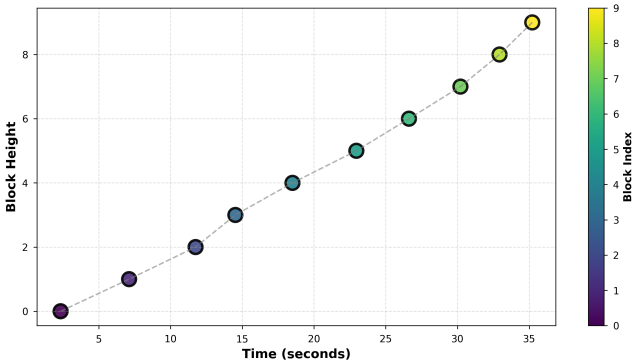

Fig. 7. Block creation timeline showing linear growth under PoA^2 consensus.

E. Overall System Case Studies

Table I presents overall system operational, resilience, and security metrics. The operational metrics show efficient execution of model explanation, data upload, and blockchain transaction submission. Throughput is high at 39.17 TPS, indicating strong processing capability. Explanation time is low, showing that SHAP generation does not create bottlenecks. Upload and submission times remain minimal, meaning the system can quickly serialize and commit results to PureChain. The efficiency gain, Mean Time To Repair (MTTR) value of 0.33, suggests moderate improvement in recovery speed across operations. Mean detection time is low, indicating fast threat identification. The MTTR value of 0.48 suggests moderate time to restore functionality after disruptions.

Availability is zero due to simulation conditions, meaning no uptime window was measured. Explanation stability is high at 0.98, meaning interpretability remains consistent across repeated samples. The attack detection rate is fair at 0.67, meaning two-thirds of malicious events were correctly identified. The false-positive rate is high at 0.58, indicating that many

TABLE I
SYSTEM SECURITY, RESILIENCE, AND OPERATIONAL METRICS

Metric	Value
Operational Metrics	
Throughput (TPS)	39.174
Explain Time Mean	0.01525
Upload Time Mean	0.00348
Submission Time Mean	0.00000395
Efficiency Gain MTTR	0.33333
Resilience Metrics	
Detection Time Mean	0.01525
MTTR Mean	0.48378
Availability	0.0
Explanation Stability Proxy	0.98665
Security Metrics	
Attack Detection Rate	0.67153
False Positive Rate	0.58730
False Negative Rate	0.32846
Tamper Attempts	6.0
Tamper Detected	1.0
Tamper Detection Rate	0.16666
Unauthorized Attempts	2.0
Unauthorized Blocked	2.0
Access Control Efficacy	1.0
Explainability Fidelity Corr.	0.98265

regular events were incorrectly flagged. The false negative rate is also significant at 0.32. Tamper attempts reached six, with only one detected, yielding a low tamper detection rate. Unauthorized attempts were successfully blocked, demonstrating strong access controls. The explainability fidelity score of 0.98 indicates that explanations remain firmly aligned with the underlying model behavior.

V. CONCLUSION

The integration of XAI and blockchain in industrial IoT systems presents both unprecedented opportunities and critical challenges. When synergized with robust cybersecurity and transparent governance, machine learning can catalyze a new generation of intelligent, resilient systems. Drawing on our foundational work in hybrid deep learning, blockchain-enhanced intrusion detection, and federated model aggregation, this study presents a coherent framework for secure industrial operations. Through structured experiments, this work provides actionable insights and replicable templates for industry adoption.

Future work will refine the ML models to minimize false positives and negatives, improve explanation fidelity through more advanced XAI methods, and strengthen system security with additional protective layers. Incorporating continuous learning mechanisms will further enhance adaptability to evolving industrial cyber threats while preserving both robustness and interpretability.

ACKNOWLEDGMENT

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (IITP-2026-RS-2020-II201612, 40%), the Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2018R1A6A1A03024003, 30%), by the Institute of Information & Coummunications Technology Planning & Evaluation (IITP)-ITRC(Information Technology Research Center) grant funded by the Korea government(Ministry of Science and ICT)(IITP-2026-RS-2024-00438430 30%)

REFERENCES

[1] Y. Pang, T. Huang, and Q. Wang, "AI and Data-Driven Advancements in Industry 4.0," *Sensors*, vol. 25, no. 7, 2025.

[2] L. A. C. Ahakonye, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Trees Bootstrap Aggregation for Detection and Characterization of IoT-SCADA Network Traffic," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 4, pp. 5217–5228, 2024.

[3] K. Kuchar and R. Fujdiak, "Analyzing Anomalies in Industrial Networks: A Data-Driven Approach to Enhance Security in Manufacturing Processes," *Computers & Security*, vol. 153, p. 104395, 2025.

[4] M. A. Rahman, M. F. Shahrior, K. Iqbal, and A. A. Abushaiba, "Enabling Intelligent Industrial Automation: A Review of Machine Learning Applications with Digital Twin and Edge AI Integration," *Automation*, vol. 6, no. 3, 2025.

[5] A. T. Rosário and J. C. Dias, "Illuminating Industry Evolution: Reframing Artificial Intelligence Through Transparent Machine Reasoning," *Information*, vol. 16, no. 12, 2025.

[6] C. I. Nwakanma, L. A. C. Ahakonye, J. N. Njoku, J. C. Odirichukwu, S. A. Okolie, C. Uzondu, C. C. Ndubuisi Nweke, and D.-S. Kim, "Explainable Artificial Intelligence (XAI) for Intrusion Detection and Mitigation in Intelligent Connected Vehicles: A Review," *Applied Sciences*, vol. 13, no. 3, 2023.

[7] L. A. C. Ahakonye, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, "Machine Learning Explainability for Intrusion Detection in the Industrial Internet of Things," *IEEE Internet of Things Magazine*, vol. 7, no. 3, pp. 68–74, 2024.

[8] L. A. C. Ahakonye, C. I. Nwakanma, and D.-S. Kim, "Tides of Blockchain in IoT Cybersecurity," *Sensors*, vol. 24, no. 10, p. 3111, 2024.

[9] H. Ibrahim, J. Kim, and U. A. Bukar, "Leveraging blockchain technology for trustworthy information dissemination in nigerian networks," *The Journal of Contents Computing*, vol. 5, no. 2, pp. 727–753, 2023.

[10] K. N. Singh and A. K. Singh, "An Integrated Framework of Blockchain and Federated Learning with Explainable AI for Enhanced Security of IoT Healthcare Systems," *International Journal of Information Technology*, pp. 1–12, 2025.

[11] L. Ofusori, T. Bokaba, and S. Mhlongo, "Explainability and Interpretability of Artificial Intelligence Use in Cybersecurity," *Discover Computing*, vol. 28, no. 1, pp. 1–23, 2025.

[12] M. Zolanvari, Z. Yang, K. Khan, R. Jain, and N. Meskin, "TRUST XAI: Model-Agnostic Explanations for AI With a Case Study on IIoT Security," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 2967–2978, 2023.

[13] L. A. C. Ahakonye, C. I. Nwakanma, J. M. Lee, and D. S. Kim, "Purechain-Enhanced Federated Learning for Dynamic Fault Tolerance and Attack Detection in Distributed Systems," *High-Confidence Computing*, p. 100354, 2025.

[14] K. Belgada and L. El Abbadi, "Blockchain and Industrial Traceability: Insights from a Systematic Literature Review Within Industry 4.0 Contexts," *Engineering Proceedings*, vol. 112, no. 1, 2025.

[15] I. B. Ababio, J. Bieniek, M. Rahouti, T. Hayajneh, M. Aledhari, D. C. Verma, and A. Chehri, "A Blockchain-Assisted Federated Learning Framework for Secure and Self-Optimizing Digital Twins in Industrial IoT," *Future Internet*, vol. 17, no. 1, 2025.

[16] H. A. Tahir, W. Alayed, W. U. Hassan, and A. Haider, "A Novel Hybrid XAI Solution for Autonomous Vehicles: Real-Time Interpretability Through LIME–SHAP Integration," *Sensors*, vol. 24, no. 21, 2024.

[17] H. Mohamed, N. Koroniotis, F. Schiliro, and N. Moustafa, "IoT-CAD: A comprehensive Digital Forensics Dataset for AI-Based Cyberattack Attribution Detection Methods in IoT Environments," *Ad Hoc Networks*, vol. 174, p. 103840, 2025.