PureChain Closed-Loop Intrusion Detection and Real-Time Recovery for Industrial IoT

Hamza Ibrahim, Love Allen Chijioke Ahakonye, *Member, IEEE*, Jae-Min Lee, *Member, IEEE*, and Dong-Seong Kim, *Senior Member, IEEE*

***Abstract*—The Industrial Internet of Things (IIoT) has transformed critical infrastructure but has also introduced severe security vulnerabilities, with breaches capable of causing catastrophic physical and operational damage. While blockchain technology offers a promising foundation for tamper-proof logging, existing platforms are often ill-suited for IIoT due to high latency, low throughput, and excessive energy consumption. Furthermore, most current research treats intrusion detection, secure logging, and system recovery as isolated components, lacking a unified framework for autonomous, verifiable resilience. To bridge this critical gap, this article introduces PureChain, a holistic, secure, and resilient ecosystem. PureChain integrates a custom lightweight blockchain with a deep learning-based intrusion detection system (IDS) and a novel verifiable recovery protocol, creating a closed-loop security model. The framework leverages a novel proof-of-authority and association (PoA^2) consensus mechanism, achieving high throughput (16.82 TPS), low latency (0.0594 s), and minimal energy consumption (12.43 W), demonstrating suitability for resource-constrained IIoT environments compared to general-purpose platforms like Ethereum and Hyperledger, which are optimized for different use cases. Upon intrusion detection by optimized models like XGBoost (99.87% accuracy), immutable blockchain logs actively trigger and cryptographically attest to infrastructure-enforced recovery actions such as device isolation via software-defined network (SDN) switches or state rollback through hardware management controllers. Extensive evaluation on benchmark IIoT datasets (IoT-CAD and IoTForge) demonstrates a detection-to-recovery success rate of up to 98.59% while maintaining 100% data integrity. PureChain establishes a new paradigm that unifies real-time threat intelligence, blockchain-based trust, and provable autonomous recovery for next-generation IIoT security.**

***Index Terms*—Blockchain-based logging, Industrial Internet of Things (IIoT) security, proof-of-authority and association (PoA^2), PureChain, verifiable recovery.**

Received 16 February 2026; accepted 5 March 2026. Date of publication 10 March 2026; date of current version 25 May 2026. This work was supported in part by the Innovative Human Resource Development for Local Intellectualization Program through Institute for Information and Communications Technology Planning and Evaluation (IITP) funded by Korea Government Ministry of Science and ICT (MSIT) under Grant IITP-2026-RS-2020-II201612 (25%); in part by the Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by Ministry of Education, Science and Technology (MEST) under Grant 2018R1A6A1A03024003 (25%); in part by MSIT, South Korea, through the Information Technology Research Center (ITRC) Support Program under Grant IITP-2026-RS-2024-00438430 (25%); and in part by the Basic Science Research Program through NRF funded by the Ministry of Education under Grant RS-2026-25431637 (25%). *(Corresponding author: Dong-Seong Kim.)*

Hamza Ibrahim and Jae-Min Lee are with the Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi 39177, South Korea (e-mail: hamza@kumoh.ac.kr; ljmpaul@kumoh.ac.kr).

Love Allen Chijioke Ahakonye is with the ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi 39177, South Korea (e-mail: loveahakonye@kumoh.ac.kr).

Dong-Seong Kim is with the Department of IT Convergence Engineering and NSLab Company Ltd., Kumoh National Institute of Technology, Gumi 39177, South Korea (e-mail: dskim@kumoh.ac.kr).

Digital Object Identifier 10.1109/JIOT.2026.3672474

I. Introduction

THE Industrial Internet of Things (IIoT) is revolutionizing critical infrastructure sectors, including smart manufacturing, energy grids, and transportation, by enabling unprecedented automation, data exchange, and efficiency [1], [2]. This convergence of cyber–physical systems, however, dramatically expands the attack surface, exposing vital industrial processes to sophisticated cyber threats [3]. Unlike conventional IT systems, security breaches in IIoT can lead to catastrophic physical damage, costly operational downtime, and significant risks to public safety [4], [5], [6].

A fundamental challenge in securing IIoT ecosystems lies in ensuring the integrity of system logs and the resilience of operational technology (OT) [7], [8], [9]. Logs that chronicle device states, commands, and process data are crucial for forensic analysis and intrusion detection [10], [11]. However, traditional centralized logging mechanisms are vulnerable to single points of failure and susceptible to tampering or deletion by attackers seeking to erase evidence, as highlighted in recent IIoT security analyses [12] (see Fig. 1). This highlights trust in the very data needed for incident response.

Blockchain technology has emerged as a promising solution to this trust problem, offering decentralization, immutability, and cryptographic verifiability for creating tamper-resistant audit trails [13], [14]. As illustrated in Fig. 2, several studies have proposed blockchain-based architectures for IIoT. For instance, Ahmad et al. [15] designed a blockchain-based authentication scheme for IoT data storage, while Kalapaaking et al. [16] used a private blockchain for access control in smart factories. Surveys further highlight blockchain's growing role in fortifying IIoT security across various layers [13], [17].

Despite this promise, mainstream blockchain platforms like Ethereum and Hyperledger face significant limitations, namely, high latency, low throughput, and substantial energy consumption, making them challenging to deploy directly in high-frequency, resource-constrained IIoT applications without significant optimization [18], [19]. Consensus mechanisms like proof-of-work (PoW) and PoS are computationally expensive, while proof-of-authority (PoA) risks excessive centralization [19], [20], [21]. Furthermore, a critical research gap persists; existing solutions primarily focus on isolated aspects such as data integrity [15], access control [16], or intrusion detection [22]. They lack a consolidated, closed-loop architecture that seamlessly links real-time anomaly detection with immutable logging and, crucially, autonomous, verifiable

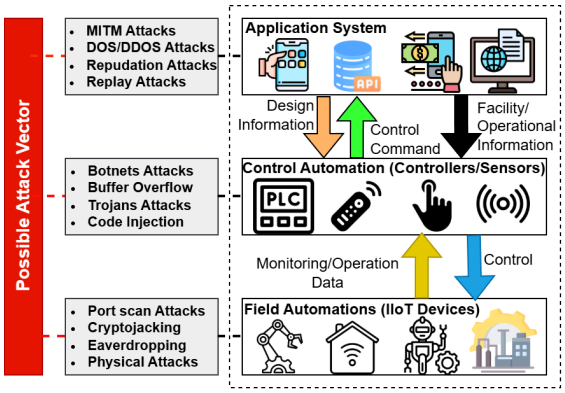

Fig. 1. IIoT architecture and possible major cyberattacks.

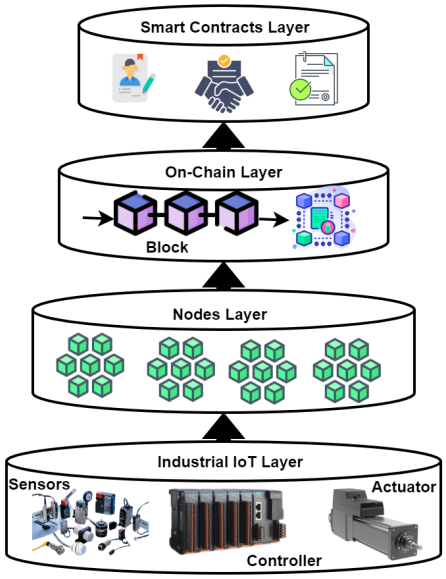

Fig. 2. Blockchain application for industrial IoT.

recovery actions. As emphasized in [23], the ability to detect an anomaly must be intrinsically linked to a proven capacity for self-healing to ensure operational continuity.

To overcome these limitations, this study proposes PureChain, a transaction-layer blockchain architecture designed to eliminate block-induced delays and provide deterministic finality through a network of trusted validator nodes. By addressing the long-standing blockchain "quadlemma" of decentralization, security, scalability, and cost [24], [25], PureChain achieves a balanced and efficient design suitable for IIoT environments [26], [27]. The proposed secure and resilient IIoT ecosystem integrates a custom blockchain (PureChain), a deep learning-based intrusion detection mechanism, and a verifiable recovery protocol within a unified framework. The principal innovation of PureChain lies in its closed-loop security architecture, in which the blockchain ledger evolves from a passive forensic repository into an active enforcement mechanism for system resilience [19], [28], [29]. Specifically, once an intrusion alert is validated using the proposed proof-of-authority and association (PoA^2) consensus mechanism, the framework autonomously triggers and immutably records predefined recovery actions such as device isolation (enforced at the network infrastructure level) or system state rollback (triggered via out-of-band management controllers), thereby establishing a verifiable and auditable linkage between intrusion detection and mitigation. The key contributions of this work are as follows.

1) We propose a novel, lightweight blockchain architecture tailored for IIoT, integrating the PoA^2 consensus mechanism with a formally defined association score based on validator uptime, response time, reputation, and load balancing to achieve high throughput (16.82 TPS), low latency (0.0594 s), and minimal energy consumption (12.43 W).
2) We design and formalize a verifiable recovery protocol that uses consensus-validated blockchain state to autonomously trigger and cryptographically attest to corrective actions. Critically, recovery is enforced at the infrastructure level (software-defined network (SDN) switches and hardware management controllers) rather than relying on compromised device compliance, bridging the gap between detection and provable resilience.
3) We develop a holistic closed-loop security framework that integrates optimized machine learning models (e.g., XGBoost achieving 99.87% accuracy with class imbalance handling via stratified sampling and scale_pos_weight) with the PureChain blockchain, enabling real-time, auditable threat response.
4) We implement a comprehensive prototype and perform extensive evaluation on benchmark IIoT datasets (IoT-CAD and IoTForge), including ablation studies, robustness analysis against adversarial perturbations, and cross-dataset generalization. Results demonstrate that PureChain maintains 100% data integrity while achieving a detection-to-recovery success rate of up to 98.59%, addressing critical gaps in existing systems that lack integrated recovery.

To the best of our knowledge, PureChain is the first framework to seamlessly integrate this trifecta of high-performance detection, efficient tamper-proof logging, and verifiable, autonomous recovery into a unified architecture that meets stringent IIoT constraints. The remainder of this article is structured as follows. Section II provides a critical analysis of related work. Section III details the PureChain system model and protocols. Section IV presents the experimental evaluation and comparative analysis. Finally, Section V concludes this article and suggests future directions.

II. Background and Related Work

This section provides a critical analysis of recent advancements in IIoT security, focusing on the integration of blockchain and machine learning. We identify key trends and, more importantly, highlight the specific limitations of current approaches that motivate the design of PureChain.

A. Blockchain for IIoT Security: Progress and Limitations

Blockchain's inherent properties of decentralization and immutability have made it a focal point for enhancing trust in IIoT. Research has evolved from conceptual proposals to specific architectural implementations. For instance, Poorazad and Ghorbani [22] combined deep learning-based intrusion detection with blockchain in SDN-enabled IIoT environments,

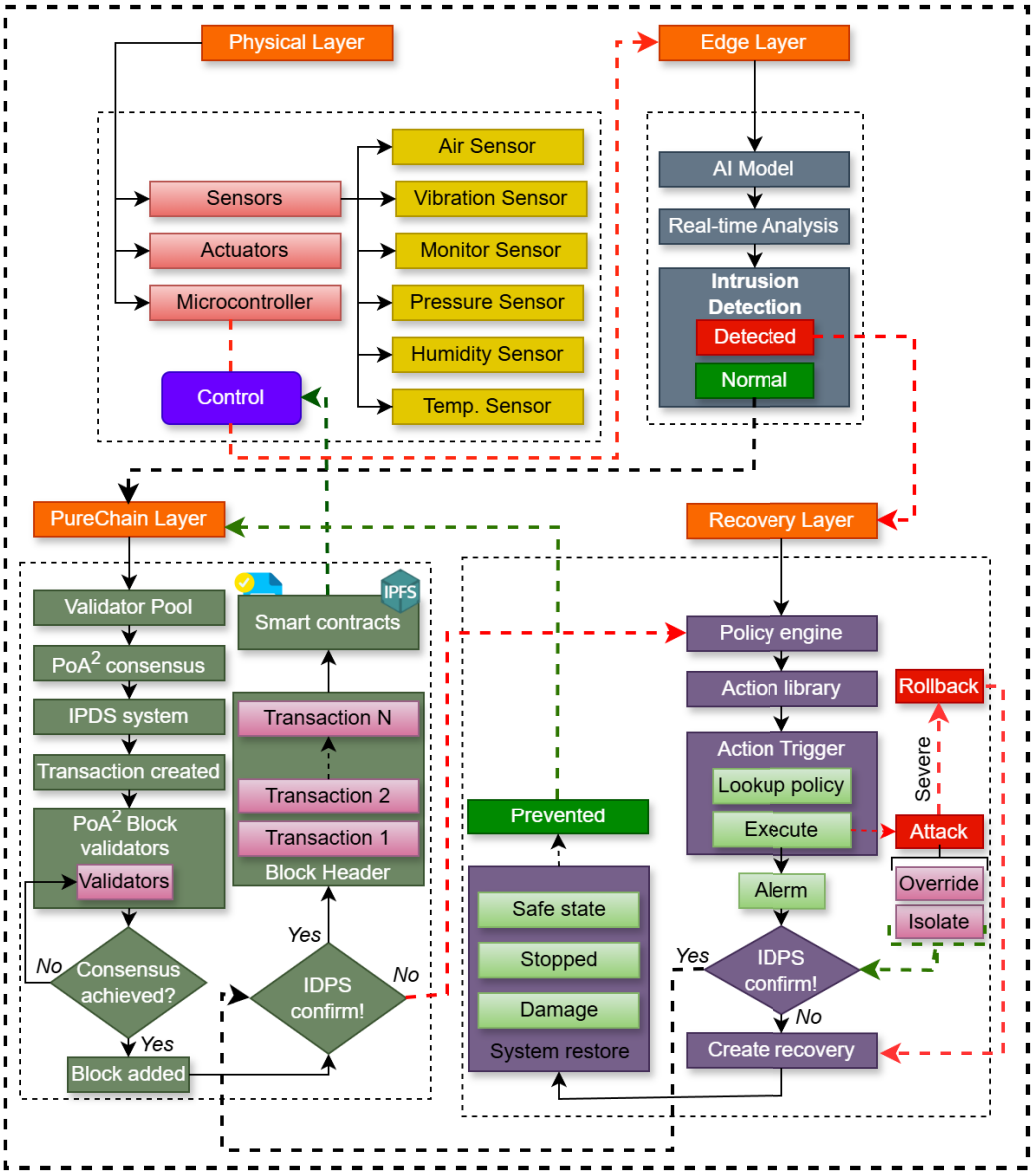

Fig. 3. End-to-end operational workflow of the PureChain framework. Data flows from physical layer sensors to edge layer for AI-based intrusion detection. Validated alerts are processed by PureChain Layer via PoA^2 consensus, triggering verifiable recovery actions enforced at the infrastructure level (SDN switches and management controllers) upon IDPS confirmation, with verification tokens returned to the blockchain to close the loop.

improving detection accuracy but treating the blockchain primarily as a secure storage backend without active recovery functions. Similarly, Maurya et al. [30] proposed a decentralized architecture for device authentication using smart contracts and IPFS, focusing on access control but lacking mechanisms for real-time response to detected breaches.

Recent works have sought to optimize blockchain for IoT constraints. Zhang et al. [31] proposed a sharded blockchain for scalable logging, achieving higher throughput. Chen et al. [32] combined federated learning with blockchain for privacy-preserving anomaly detection. While these works address scalability and privacy, a common shortcoming is their treatment of the blockchain as a passive ledger. They do not leverage its consensus-validated state to actively orchestrate system-level responses, leaving a disconnect between detection and mitigation. Other studies, like Stodt's Zero Trust blockchain architecture [33] and Hashi's BLOX-Trust framework [34], integrate identity management and anomaly

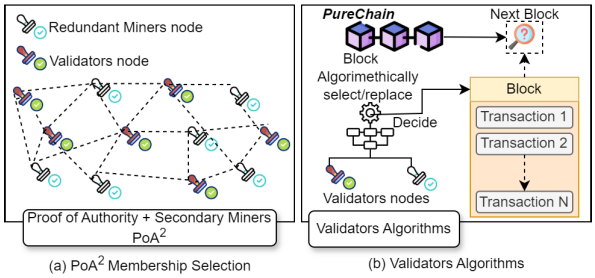

Fig. 4. PoA^2 validator selection. (a) VRF-based weighted selection process. (b) Active validator consensus flow.

detection, moving toward more proactive security. However, when present, their recovery mechanisms are not deeply integrated with the blockchain's trust mechanism; the ledger does not formally attest to the execution and outcomes of recovery actions.

B. Intrusion Detection and Recovery: A Disjointed Landscape

Recent advances in intrusion detection systems (IDSs) for IIoT have demonstrated remarkable progress across diverse architectural paradigms. Li et al. [35] showed that Transformer-based models can capture long-range dependencies in network traffic, achieving strong performance in in-vehicle intrusion detection using BERT architectures. Similarly, Gueriani et al. [36] employed hybrid convolutional neural network (CNN)-long short-term memory (LSTM) frameworks to obtain high accuracy on contemporary datasets such as CICIoT2023 and CICIDS2017. Islam et al. [37] extended this direction by introducing automated machine learning (AutoML) combined with meta-learning for zero-touch network environments, integrating explainable artificial intelligence (AI) mechanisms to improve transparency and model interpretability.

Edge-centric intrusion prevention has also gained traction in resource-sensitive IIoT settings. Algarni et al. [38] proposed edge-based threat prioritization for smart grids using modified LightGBM and one-class SVM models, enabling behavior-aware response at the network edge. Waqas and Tariq [39] conducted comprehensive benchmarking of deep learning models, including CNN, LSTM, and bidirectional long short-term memory (BiLSTM), across multiple IoT datasets (BoTIoT, CICIoT, and TONIoT), consistently reporting detection accuracies above 98% in controlled environments. In parallel, Srinivasan and Senthilkumar [40] explored the integration of reinforcement learning with blockchain to support dynamic threat prevention, enabling real-time adaptive response while maintaining data integrity through distributed ledger technology.

Routing-specific and resource-constrained IoT scenarios have motivated specialized detection architectures. Hafsa et al. [41] demonstrated that cross-layer feature analysis combined with gradient boosting algorithms such as CatBoost and XGBoost can detect RPL attacks with 99% accuracy while maintaining false positive rates below 1%. For wireless sensor networks, Singh et al. [42] introduced the SS-LSACNN architecture with correlation-based synthetic minority oversampling technique (SMOTE) to address data imbalance, achieving robust distributed denial of service (DDoS) detection performance under constrained computational settings.

Despite these advances in detection accuracy and architectural innovation, a consistent limitation across existing IDS frameworks is their isolation of the detection phase. High-performance models typically generate alerts or logs but rarely initiate automated, verifiable recovery processes. Recovery and resilience mechanisms in IIoT remain underexplored and often disconnected from the core security loop. Sankpal and Deshmukh [43] highlight the need for decentralized recovery protocols, yet their survey does not present concrete blockchain-attested implementations. Similarly, Prakash and Kumar [44] describe real-time monitoring frameworks that omit immutable audit trails required for forensic verification and regulatory compliance in industrial environments. This exposes a critical gap. Even when attacks are detected with high accuracy, the system's ability to provably and autonomously recover is not guaranteed.

C. Identified Research Gap and Our Position

The analysis of recent literature, synthesized in Table I, reveals a consistent pattern; most solutions excel in one or two domains (e.g., detection, logging, or access control) but fail to provide a cohesive, closed-loop system. The critical missing link is a mechanism that uses the trusted, immutable state of a blockchain not just to record events, but also to authorize and verify autonomous recovery actions in real time. This lack of integration means IIoT systems remain vulnerable in the crucial window between detection and manual intervention, and lack forensic proof that recovery was executed correctly.

Our proposed framework is designed to bridge this exact gap. Unlike prior works, it unifies high-performance machine learning (ML)-based detection (leveraging insights from comparative studies such as [39] and [45]), a lightweight blockchain optimized via PoA^2 consensus (addressing scalability issues noted in [31]), and a formal, verifiable recovery protocol. This creates an end-to-end framework where detection automatically, immediately, and provably triggers mitigation, with every step immutably logged for audit. This holistic approach to IIoT resilience is the key differentiator of our work.

III. System Model

The proposed ecosystem is a formally defined, closed-loop security framework that integrates the PureChain blockchain ledger with deep learning-based intrusion detection and prevention and a verifiable state recovery protocol. This section provides a rigorous specification of the system architecture, threat model, and core protocols.

A. Architecture and Components

The proposed architecture, illustrated in Fig. 3, operates on a hybrid edge–fog computing model. The system is modeled as a tuple $\mathcal{S} = (\mathcal{P}, \mathcal{E}, \mathcal{F}, \mathcal{R})$, representing the four logical layers.

1) *Physical Layer ($\mathcal{P}$):* It comprises the set of IIoT devices $\mathcal{D} = \{d_1, d_2, \ldots, d_n\}$. Each device d_i has a state $s_i(t) \in \mathcal{S}_i$ at time t and generates a continuous multivariate data stream $\mathbf{x}_i(t) \in \mathbb{R}^m$ representing sensor readings and control commands.
2) *Edge Intelligence Layer ($\mathcal{E}$)*: It consists of edge nodes $\mathcal{N}_{edge}$. Each node hosts an intrusion detection model $f_{edge} : \mathbb{R}^m \to \{0, 1\}$, where 1 signifies an intrusion. To address data imbalance during training, we employ stratified sampling and class weighting techniques. Upon detection, it creates an *intrusion alert* transaction $TX_{alert} = \langle d_i, \mathbf{x}_i(t'), H(\mathbf{x}_i(t')), \sigma_{edge} \rangle$, where H is a cryptographic hash function and σ_{edge} is a digital signature.
3) *PureChain and Control Layer ($\mathcal{F}$):* It comprises a set of more powerful fog nodes $\mathcal{N}_{fog}$. A subset $\mathcal{V} \subset \mathcal{N}_{fog}$, with $|\mathcal{V}| = k$, acts as the validator pool for the PureChain ledger $\mathcal{L}$. The ledger is a cryptographically linked chain of blocks $\mathcal{L} = (B_0, B_1, \ldots, B_l)$, where each block $B_i = (H(B_{i-1}), TXs, nonce)$. The core of this layer is the PoA^2 consensus mechanism. Let $\mathcal{V}_{active} \subseteq \mathcal{V}$ be the set of active validators for a given round. The consensus function Λ is defined as follows:

$$\Lambda\left(\mathcal{V}_{active}, \mathbf{TX}_{pool}\right) \to B_{new} \tag{1}$$

TABLE I
CRITICAL ANALYSIS OF RELATED WORKS AND POSITIONING OF THE PROPOSED FRAMEWORK

Ref.	Approach	Strengths	Limitations / Gaps	How Proposed Framework Addresses This
			Blockchain & IIoT Security Integration	
[22]	DL + Blockchain IDS	High detection accuracy in SDN-IIoT.	Blockchain used as passive log; no integrated recovery mechanism.	Uses blockchain as active resilience enforcer; integrates verifiable recovery protocol.
[30]	Decentralized Auth (Smart Contracts)	Secure, automated access control.	Focuses on pre-access trust, not post-breach response or real-time audit.	Adds real-time, blockchain-attested response to post-breach alerts.
[33]	Zero Trust Blockchain	Integrates identity	No tight coupling between ML detection	Tightly couples optimized ML detection
[34]	BLOX-Trust (Zero Trust)	High anomaly detection accuracy.	Recovery actions lack blockchain-based verification and audit trail.	Recovery actions are triggered by and logged on-chain, creating a verifiable audit trail.
[31]	Sharded Lightweight Blockchain	High throughput for scalable logging.	Focuses on logging scalability without linking logs to active response.	Leverages efficient PoA^2 consensus for logging and uses logs to trigger recovery actively.
[32]	Federated Learning + Blockchain	Privacy-preserving collaborative detection.	Framework lacks a mechanism for autonomous, verifiable system recovery.	Introduces a verifiable recovery protocol that can leverage federated insights.
			Intrusion Detection Systems (ML/DL Based)	
[36]	Hybrid CNN-LSTM	High accuracy on IoT datasets.	Standalone detection model; no integration with security orchestration or audit.	Integrates such high-performance models as the detection engine within the closed-loop framework.
[45]	ML Model Comparison	Identifies XGBoost, RF as top performers.	Study is comparative only; no proposed unified security framework.	Adopts top-performing models identified by such studies for our detection layer.
[39]	DL Benchmarking	Comprehensive evaluation across multiple scenarios.	Focuses on detection metrics; does not advance system resilience.	Uses robust detection as the first step in a broader resilience pipeline (detect-log-recover).
[35]	Cloud-Collaborative BERT for IVN	High performance on in-vehicle networks; sliding window feature extraction.	Domain-specific (vehicles); detection primary goal without autonomous response.	Generic framework applicable to IVN with strong focus on response verification.
[40]	CNN + Blockchain-assisted RL	Real-time learning for prevention; blockchain for data integrity.	RL for prevention novel, but recovery actions not formally audited on-chain.	Recovery actions cryptographically attested and logged with verification tokens.
[37]	AutoML + Meta-Learning + XAI	Addresses model adaptability and transparency in zero-touch networks.	Focuses on detection transparency; no tamper-proof system for response execution.	XAI principles integrable in future work; current focus on verifiable execution.
[41]	Cross-layer features + CatBoost	99% detection rate for RPL attacks; prevention algorithm included.	Prevention lacks immutable, verifiable audit trail for actions taken.	Every prevention action recorded on PureChain ledger with verifiable proof token.
[38]	Edge-computing + Modified LGBM/SVM	Edge-based detection with threat prioritization for smart grids.	Response implied without tamper-proof log linking priority to action.	Logs priority and triggered action on-chain, creating auditable incident response chain.
[42]	SS-LSACNN + CC-SMOTE	High DDoS detection accuracy; explicitly addresses data imbalance.	Focuses on detection for specific attack; lacks system-wide resilience mechanism.	Adopts imbalance techniques as first step in broader automated resilience pipeline.
			Recovery & Resilience	
[43]	Survey on Blockchain-AI fusion	Highlights need for decentralized recovery.	Conceptual discussion; no implementation or protocol for verifiable recovery.	Provides concrete implementation of blockchain-verified recovery protocol.
[44]	ML Anomaly Detection Framework	Includes real-time monitoring.	Recovery and logging lack immutability and verifiable proofs.	Ensures all recovery actions immutable with cryptographic proof of execution.

where $\mathbf{TX}_{pool}$ is the set of pending transactions. A validator $v_j \in \mathcal{V}_{active}$ is selected based on a verifiable random function (VRF) weighted by an association score $A(v_j)$, defined as

$$A\left(v_j\right) = \alpha \cdot U_j + \beta \cdot \left(1/L_j\right) + \gamma \cdot R_j - \delta \cdot C_j \tag{2}$$

where U_j is the historical uptime, L_j is the average response latency, R_j is the reputation score (decreased for malicious behavior), and C_j is the recent consensus participation count to ensure load balancing. The weights α, β, γ, and δ are system parameters with $\alpha + \beta + \gamma + \delta = 1$. The system maintains a redundant pool such that $|\mathcal{V}| > k$, ensuring that if a validator v_j is compromised and deemed $v_j^{malicious}$, it is removed and a redundant node v_r is activated in Equation (3) and Fig. 4.

$$\mathcal{V}_{active} \leftarrow \left(\mathcal{V}_{active} \setminus \left\{v_j^{malicious}\right\}\right) \cup \{v_r\}. \tag{3}$$

4) *Recovery and Verification Layer ($\mathcal{R}$):* This layer hosts the *recovery orchestrator*, a state machine that monitors $\mathcal{L}$. For a new block B_l containing a validated TX_{alert}, it executes a recovery function Ψ. Critically, recovery actions are enforced at the infrastructure level, not by compromised devices themselves. The entire process ensures a deterministic and verifiable state transition for the IIoT system. The system moves from a potentially compromised state $\mathbf{S}(t) = [s_1(t), \ldots, s_n(t)]$ to a recovered, trusted state $\mathbf{S}(t + \Delta t)$, with the entire sequence of events $\Gamma = (\mathbf{x}_i, TX_{alert}, B_l, \Psi, \pi_{rec}, TX_{rec})$ immutably logged on $\mathcal{L}$ for audit, forensics, and compliance. The recovery function Ψ is a critical component, defined for a device d_i in the following equation:

$$\Psi(d_i, a) = \begin{cases} \Psi_{\text{isolate}}\left(d_i, \mathcal{N}_{\text{switch}}\right), & a = \texttt{ISOLATE} \\ \Psi_{\text{rollback}}\left(d_i, s_i^{\text{golden}}\right), & a = \texttt{ROLLBACK} \\ \Psi_{\text{override}}\left(d_i, cmd_{\text{correct}}\right), & a = \texttt{OVERRIDE} \end{cases} \tag{4}$$

where $\Psi_{rollback}$ reverts device d_i to a known-good state s_i^{golden} via out-of-band management controllers [e.g., baseboard management controller (BMC)/intelligent platform management interface (IPMI)] that force reload of golden image; $\Psi_{isolate}$ configures the network switch $\mathcal{N}_{switch}$ to drop all packets to/from d_i at the hardware

level, independent of device compliance; and $\Psi_{override}$ issues a correct command $cmd^{correct}$ to neutralize a malicious one through trusted gateway proxies. The entire process ensures a deterministic state transition for the IIoT system, from a potentially compromised state $\mathbf{S}(t) = [s_1(t), \ldots, s_n(t)]$ to a recovered, trusted state $\mathbf{S}(t + \Delta t)$, with the entire sequence of events $(\mathbf{x}_i, TX_{alert}, B_l, \Psi, TX_{rec})$ immutably logged on $\mathcal{L}$ for audit and analysis.

B. Complexity Analysis of PoA^2 Consensus

The time complexity of the PoA^2 consensus round is dominated by the VRF computation for leader selection and the k-of-n signature aggregation for block commitment. For a validator pool of size $|\mathcal{V}| = n$ and an active set of size k, leader selection via VRF is $O(1)$ per validator, resulting in $O(n)$ for the pool. The subsequent multisignature aggregation for k validators is typically $O(k)$ using BLS signature schemes. With k being a small constant (e.g., $k = 5$), the overall consensus complexity per block is effectively $O(n)$, which is linear in the validator pool size. This is a significant improvement over PoW's $O(2^\kappa)$ cryptographic puzzle solving or baseboard management controller (BFT)-based protocols' $O(n^2)$ communication overhead, making PoA^2 highly suitable for low-latency IIoT networks.

C. Threat Model and Formal Security Properties

We operate within the Dolev–Yao adversarial model [46], [47] extended for IIoT. The adversary $\mathcal{A}$ controls a subset of entities and aims to compromise the confidentiality, integrity, and availability (CIA) triad. In our model, confidentiality refers to the property that sensitive data, including device states, control commands, and logged transactions, are not disclosed to unauthorized entities. This is enforced through permissioned blockchain access and encryption of transaction payloads. PureChain is designed to preserve the following properties.

1) *Data Integrity ($\mathcal{I}$):* For any transaction TX logged in block B_i, it is computationally infeasible for $\mathcal{A}$ to produce an alternate chain $\mathcal{L}'$ where TX is altered or removed

$$\Pr\left[\mathcal{A}\text{succeeds in breaking } \mathcal{I}\right] \leq \epsilon(\kappa) \tag{5}$$

where ϵ is a negligible function in the security parameter κ.

2) *Liveness ($\mathcal{L}_v$):* Despite $\mathcal{A}$ compromising up to $f < (|\mathcal{V}_{active}|)/2$ validators, the consensus protocol Λ will eventually produce a new block B_{new}

$$\forall t, \exists t' > t : \Lambda\left(\mathcal{V}_{active}, \mathbf{TX}_{pool}\right) \rightarrow B_{new}\text{at time } t'. \tag{6}$$

The redundant validator pool and the fault detection mechanism in PoA^2 maintain this.

3) *Verifiable Recovery ($\mathcal{V}_\mathcal{R}$):* For any recovery action $a = \Psi(d_i)$ triggered by a validated $TX_{alert} \in B_l$, a verifiable proof of its execution π_{rec} exists and is logged in a subsequent block B_{l+c}

$$\forall a, \exists \pi_{rec} : \text{Verify}(\pi_{rec}, a, B_l) = \text{True} \wedge \pi_{rec} \in B_{l+c}. \tag{7}$$

D. Core PureChain Verifiable Recovery Protocol

The closed-loop security of PureChain is enacted by the continuous execution of a verifiable recovery protocol, formalized in Algorithm 1. This protocol ensures that a consensus-validated intrusion alert automatically and provably triggers a corrective action in the physical layer, creating an immutable chain from detection to mitigation. The recovery function Ψ is defined as a set of atomic, idempotent actions mapped to specific threat types through a policy lookup $\mathcal{P} : TX_{alert} \rightarrow a$. For a device d_i and an alert transaction TX_{alert}, the action $a = \Psi(d_i, TX_{alert})$ is selected from the following primitives.

1) $\Psi_{isolate}(d_i, \mathcal{N}_{switch})$*:* It commands a SDN switch $\mathcal{N}_{switch}$ to immediately drop all packets to and from the compromised device d_i at the hardware forwarding level. This is the primary response to malware propagation or a compromised endpoint, enforced independently of device cooperation.
2) $\Psi_{rollback}(d_i, s_i^{golden})$*:* It reverts the state of d_i (e.g., a programmable logic controller (PLC) or controller) to a known-good, secure state s_i^{golden} stored in a secure, immutable repository. This action is triggered via out-of-band management interfaces (e.g., BMC and IPMI) that force a hardware reset and golden image reload, ensuring execution even if the device OS is compromised.

Algorithm 1 PureChain Verifiable Recovery Protocol

Input : Validated block B_l containing transactions
Output: Recovery transaction TX_{rec} recorded on-chain
Procedure: RecoveryOrchestrator
if B_l *contains validated* TX_{alert} **then**
  $a \leftarrow \mathcal{P}(TX_{alert})$ `// Policy lookup to determine corrective action`
  $(result, r) \leftarrow$ ExecuteInfrastructureAction(a) `// Enforced by SDN switch/management controller`
  $\pi_{rec} \leftarrow \langle H(TX_{alert}), a, \text{timestamp}, \sigma_{orchestrator}, r\rangle$;
  $TX_{rec} \leftarrow$ CreateRecoveryTx(π_{rec});
  SubmitToBlockchain(TX_{rec});
  `// Log verifiable proof of recovery`
end

3) $\Psi_{override}(d_i, cmd^{correct})$*:* It issues a correct command $cmd^{correct}$ to neutralize a malicious command through trusted gateway proxies that intercept and validate control plane traffic. For example, if a malicious `VALVE_OPEN` command is detected, the orchestrator issues a `VALVE_CLOSE` command. This is critical for responding to command injection attacks in real-time control loops.

The cornerstone of verifiable recovery is the generation of a verification token, π_{rec}. This token is not merely a log entry but a cryptographic proof linking the action to its outcome. It is constructed in the following equation:

$$\pi_{rec} = \langle H(TX_{alert}), a, t, \sigma_{orchestrator}, r\rangle \tag{8}$$

where $H(TX_{alert})$ is hash of the triggering alert transaction, creating an immutable link to the cause; a is the

specific recovery action executed; t is the timestamp of action execution; $\sigma_{orchestrator}$ is the digital signature of the recovery orchestrator, providing nonrepudiation; and r is the Outcome Attestation. This is a signed confirmation from the enforcing infrastructure component (SDN switch, management controller, and gateway proxy) verifying the action's result (e.g., "`ACK: PORT_BLOCKED`" or "`STATE: GOLDEN_IMAGE_LOADED`"). The protocol execution proceeds as follows.

1) *Trigger:* The recovery orchestrator, upon the immutable addition of a validated TX_{alert} to block B_l, parses the alert and selects an action a via a policy map $\mathcal{P}$: $TX_{alert} \rightarrow a$.
2) *Execution and Attestation:* The orchestrator sends command a to the relevant infrastructure enforcer (switch, management controller, and gateway) and waits for the outcome attestation r from the enforcing component.
3) *Verification and Logging:* The orchestrator constructs π_{rec} and submits it as a new transaction TX_{rec} to the PureChain network. The consensus mechanism validates the orchestrator's signature and the logical link to TX_{alert} before appending TX_{rec} to a new block B_{l+c}.

E. AI Architecture Integration and Operational Workflow

The AI/ML subsystem implements optimized classifiers, including XGBoost, CNN, LSTM, and BiLSTM, trained on feature vectors $\mathbf{x}_i(t) \in \mathbb{R}^m$, extracted from IIoT device streams, where m denotes the feature dimensionality (e.g., $m = 61$ for dataset Windows traces). To address class imbalance in the training data, we employ stratified K-fold cross-validation to maintain class distribution across folds. For tree-based models like XGBoost, we utilize the scale_pos_weight parameter to penalize misclassification of minority classes, while for deep learning models, class weighting is applied during loss computation. Hyperparameter tuning for XGBoost employs gradient boosting with regularization parameters λ and γ, maximum tree depth $d_{\max}$, and learning rate η, optimized via cross-validation on stratified splits of the datasets.

The edge-level detection function is defined as $f_{\text{edge}} : \mathbb{R}^m \rightarrow \{0, 1\}$, and for binary classification, or $f_{\text{edge}} : \mathbb{R}^m \rightarrow \{C_1, \ldots, C_k\}$ for multiclass settings. Following comparative analysis of all four optimized models, XGBoost was selected as the deployment model for the IDPS due to its superior balance of accuracy (99.87%) and inference latency (0.000137s) in binary classification tasks, as detailed in Section IV. In the binary case, a positive detection triggers the creation of an *intrusion alert transaction* $TX_{\text{alert}} = \langle d_i, \mathbf{x}_i(t'), H(\mathbf{x}_i(t')), \sigma_{\text{edge}} \rangle$, where d_i denotes the device identifier, $H(\cdot)$ represents the SHA-256 hash function, and σ_{edge} is an ECDSA signature generated using the edge node's private key. Transaction integration into the PureChain ledger follows a deterministic state transition protocol. Upon validation through the PoA^2 consensus mechanism where leader selection probability is weighted by the association score defined in $\text{Rep}_t(v_i) = \text{Rep}_{t-1}(v_i) \cdot \delta + \alpha \cdot \text{Availability}(v_i) + \beta \cdot \text{Correctness}(v_i) - \gamma \cdot \text{LatencyPenalty}(v_i)$, where the transaction is appended to block B_l with a mean latency of 0.0594 s. The consensus time complexity is $\mathcal{O}(n)$ for a validator pool of size n, with leader selection operating in $\mathcal{O}(1)$ per validator and signature aggregation in $\mathcal{O}(k)$. Once the ledger is updated, the *recovery orchestrator* is triggered. This component operates as a state machine that maps TX_{alert} to a mitigation action $a \in \{\texttt{ISOLATE}, \texttt{ROLLBACK}, \texttt{OVERRIDE}\}$ via a policy function $P : TX_{\text{alert}} \rightarrow a$. Action execution is formalized in 4.

Each mitigation action is subject to strict temporal constraints. Specifically, Ψ_{isolate} reconfigures SDN switch flow tables within <100 ms, Ψ_{rollback} restores the device state from a cryptographically hashed golden image s_i^{golden} within 1–2 s via hardware management controller, and Ψ_{override} issues corrective commands within subsecond latency through trusted gateways, which is critical for real-time industrial control loops. Following execution, the orchestrator generates a verification token $\pi_{\text{rec}} = \langle H(TX_{\text{alert}}), a, t, \sigma_{\text{orchestrator}}, r \rangle$, where r denotes a signed attestation (e.g., `ACK:PORT_BLOCKED`) from the enforcing infrastructure component. This token is submitted as a recovery transaction TX_{rec} to *PureChain*, forming an immutable and verifiable event chain $\Gamma = (\mathbf{x}_i, TX_{\text{alert}}, B_l, \Psi, \pi_{\text{rec}}, TX_{\text{rec}})$. The end-to-end latency is bounded by $T_{\text{total}} = T_{\text{infer}} + T_{\text{IDPS}} + T_{\text{block}} + T_{\Psi}$, where $T_{\text{infer}} \in [0.00006, 0.0025]$ s (model-dependent), $T_{\text{IDPS}} \in [0.135, 0.927]$ ms, $T_{\text{block}} \approx 0.0594$ s, and $T_{\Psi} \in [0.001, 2.2]$ s. This closed-loop coordination confirms that *PureChain* satisfies the latency, auditability, and resilience requirements of resource-constrained IIoT environments.

IV. Experimental Setup and Performance Evaluation

This section outlines the implementation and performance assessment of the proposed secure blockchain framework built on trusted computing hardware. We begin by defining our evaluation methodology, baselines, and metrics to ensure clarity.

1) *Evaluation Methodology:* Our evaluation addresses three primary goals: assessing intrusion detection performance across multiple models and configurations, benchmarking blockchain platform performance for IIoT suitability, and measuring end-to-end system resilience, including recovery success rates.
2) *Baselines:* For intrusion detection, we compare XGBoost, CNN, LSTM, and BiLSTM as representative ML/DL models. For blockchain performance, we compare against Hyperledger Fabric and Ethereum (Goerli testnet) as mainstream permissioned and public platforms. For holistic system comparison, we reference recent integrated frameworks from the literature, acknowledging that direct reproduction is limited by code availability and hardware heterogeneity.
3) *Metrics:* Detection performance is evaluated using accuracy, precision, recall, $F1$-score, macro/weighted $F1$, AUC-ROC, and inference time. Blockchain performance metrics include throughput (TPS), latency (s), and energy consumption (W). System resilience metrics include detection-to-recovery success rate, end-to-end latency, and false positive rate impact on recovery actions.
4) *Hardware Setup:* All experiments were conducted on a Windows 11 workstation with 12th-generation Intel Core i5-12400F processor, 32-GB DDR4 RAM (3200 MT/s), and NVIDIA GeForce RTX 3050 GPU

(8-GB VRAM). Network bandwidth was configured at 1 Gb/s with emulated 5-ms RTT latency.

A. System Implementation

All simulations were conducted using Python 3.10, with preliminary development carried out on Google Colab and final experiments executed on a Windows 11 workstation. The experimental platform was equipped with a 12th-generation Intel Core i5-12400F processor, 32-GB DDR4 memory (3200 MT/s), and an NVIDIA GeForce RTX 3050 GPU with 8-GB VRAM, ensuring adequate computational resources for parallel model training, inference, and blockchain operations. The blockchain network was emulated using seven validator nodes, operating under a quorum threshold of five nodes to achieve consensus finality, representative of a medium-scale IIoT deployment. Blockchain functionality was implemented using the native PureChain Software Development Kit (SDK) (https://pypi.org/project/purechainlib/) developed by the Networked Systems Laboratory [48] and integrated with `web3.py` alongside a custom Python abstraction that encapsulates encrypted client data into blockchain blocks. It is important to note that all evaluations were performed in a simulated environment using publicly available benchmark datasets, rather than a physical IIoT testbed.

B. Dataset Description

The proposed framework was evaluated using two benchmark IIoT datasets: IoT-CAD [49] and IoTForge [50]. These datasets capture a range of network scales, attack patterns, and protocol types, enabling a thorough assessment across diverse industrial conditions.

1) IoT-CAD is a large-scale IoT forensics dataset for cyber-attack detection and attribution, improving on BoTIoT, ToN_IoT, and Edge-IIoTset. The dataset contains over 530 000 samples with 61 features (Windows traces) and 76 features (Linux traces), spanning seven attack classes and 14 subtypes. Class distribution is imbalanced, with normal traffic comprising approximately 45% of samples, DoS attacks 25%, and remaining attack types (probing, injection, password cracking, man-in-the-middle (MITM), and malware) comprising the remaining 30% with varying representation. Preprocessing applied correlation-based feature reduction, normalization, and redundancy removal to ensure model efficiency and clarity.
2) IoTForge Pro is a comprehensive IIoT dataset with 1 million preprocessed and 3 million raw samples, featuring 96 and 159 attributes, respectively. The dataset includes multiple attack types: DoS (18% of samples), ransomware (12%), XSS (10%), password attacks (15%), DDoS (20%), and vulnerability scans (10%), with normal traffic comprising approximately 15% of samples. This imbalance reflects real-world IIoT conditions where attack instances are less frequent than benign operations. Though synthetic, it provides balanced data and protocol diversity suitable for deep learning IDS studies. The preprocessed folder includes 1 000 000 labeled samples, while the unprocessed set contains 17 attack-specific files (e.g., ddos_tcp.csv, dos_icmp.csv, mitm_arp.csv, vuln_scan.csv, and normal.csv). IoTForge Pro thus serves as a scalable and realistic benchmark for evaluating IDS models in industrial IoT environments.

TABLE II
PERFORMANCE COMPARISON OF MACHINE LEARNING MODELS UNDER BINARY AND MULTICLASS SETTINGS (IOT-CAD DATASET)

(a) Binary Classification Results

Model	Accuracy	Precision	Recall	F1-Score	Inference Time (s)
XGBoost	0.998690	0.998714	0.999343	0.999029	0.000137
CNN	0.993508	0.991923	0.998494	0.995198	0.000060
LSTM	0.992788	0.991460	0.997892	0.994666	0.000160
BiLSTM	0.992862	0.991087	0.998385	0.994722	0.000271

(b) Multiclass Classification Results

Model	Accuracy	Precision	Recall	F1-Score	Inference Time (s)
XGBoost	0.998617	0.998846	0.998932	0.998889	0.002500
CNN	0.992346	0.991530	0.996308	0.993890	0.000076
LSTM	0.994577	0.993948	0.996738	0.995334	0.000380
BiLSTM	0.992936	0.991586	0.995693	0.993575	0.000756

C. Performance Scenario and Analysis (IoT-CAD Dataset)

Table II presents a comprehensive comparison of four machine learning models, XGBoost, CNN, LSTM, and BiLSTM, evaluated under both binary and multiclass classification scenarios on the IoT-CAD dataset. To address class imbalance, we employed stratified 70/30 train–test splits with class weighting during training. For XGBoost, scale_pos_weight was set to the ratio of negative to positive samples; for deep learning models, class weights were computed as inversely proportional to class frequencies. Across both tasks, XGBoost achieved the highest accuracy and $F1$-score (0.9990 in binary and 0.9989 in multiclass), indicating its superior capability to capture complex decision boundaries with minimal inference delay (0.0025 s). The LSTM and BiLSTM models demonstrated strong temporal learning ability, achieving $F1$-scores above 0.994 in both settings, validating their robustness in processing sequential IIoT data streams. The CNN model maintained competitive accuracy (0.9935 binary and 0.9923 multiclass) while offering the fastest inference (0.00006 s), making it well-suited for immediate edge deployments. We also computed macro-averaged $F1$-scores to verify performance across minority classes; XGBoost achieved 0.9978 macro $F1$ in binary and 0.9962 in multiclass, confirming that imbalance handling was effective. Overall, the results highlight a clear tradeoff between accuracy and computational cost; XGBoost delivers near-perfect precision at slightly higher inference times, while deep learning models like LSTM and CNN balance efficiency and adaptability for large-scale IoT environments. These findings confirm that the proposed framework can support both rapid binary anomaly detection and high-reliability fine-grained multiclass event classification.

Table III presents a comparative analysis of the proposed system under binary and multiclass classification configurations on the IoT-CAD dataset. The "Deep Learning Model" row specifically represents XGBoost, which was selected as the deployment model following the comparative analysis in

TABLE III

COMPARATIVE BINARY AND MULTICLASS PERFORMANCE EVALUATION OF SYSTEM COMPONENTS (IOT-CAD DATASET)

Component	Binary	Multiclass
Deep Learning Model (XGBoost)[1]		
Accuracy	0.871	0.804
Precision	0.992	0.802
Recall	0.813	0.810
F1-Score	0.824	0.805
Macro F1-Score	0.819	0.798
Weighted F1-Score	0.823	0.803
Inference Time (s)	0.0001	0.0008
Intrusion Detection and Prevention System (IDPS)		
Detection Accuracy	0.871	0.804
Latency (ms)	0.135	0.752
False Positive Rate (FPR)	0.85%	19.78%
Recovery System		
Detection-to-Recovery Latency (s)	1.83	1.65
Success Rate	97.47%	95.86%
Blockchain Logging		
Transaction Time (s)	0.470	0.282
Data Integrity	100.0%	100.0%
Auditability	Immutable, Verified	Immutable, Verified
Overall System		
Uptime	99.60%	99.67%
Throughput (/s)	2470.56	1951.44
Scalability	High (Edge–Fog Hybrid)	High (Edge–Fog Hybrid)

[1]XGBoost selected as deployment model based on best overall accuracy-F1 tradeoff from Table II.

Table II due to its superior balance of accuracy (99.87%) and inference efficiency. Additional macro and weighted $F1$-scores are included to demonstrate performance consistency across imbalanced classes. The binary scenario demonstrates superior predictive performance, with the deep learning model achieving an accuracy of 0.871, a precision of 0.992, and an $F1$-score of 0.824. Its inference time of 0.0001 s confirms high computational efficiency suitable for dynamic decision-making in IIoT environments. IDPS achieved low latency (0.135ms) and a minimal false positive rate (0.85%), indicating fast and reliable detection. In contrast, the multiclass configuration representing a more complex classification task maintained stable performance, achieving an accuracy of 0.804 and an $F1$-score of 0.805, while exhibiting slightly higher latency and false positives. The elevated false positive rate (19.78%) in multiclass scenarios reflects the increased complexity of distinguishing between multiple attack types. In production deployment, the policy function $\mathcal{P}$ would incorporate confidence thresholds, where low-confidence alerts trigger less disruptive actions (e.g., quarantine for observation) rather than aggressive isolation or rollback, balancing sensitivity against operational stability. The blockchain logging layer consistently preserved 100% data integrity and verified immutability across both configurations, validating the robustness of PureChain's consensus and audit mechanisms. Overall, the binary setup emphasizes high accuracy and minimal delay, making it ideal for security-critical deployments. In contrast, the multiclass setup demonstrates scalability and adaptability in complex IIoT scenarios involving multiple event types or sensor categories. Together, these results confirm the system's balanced tradeoff between precision, efficiency, and resilience across diverse operational contexts.

D. Performance Scenario and Analysis (IoTForge Dataset)

Table IV compares the performance of four machine learning models, XGBoost, CNN, LSTM, and BiLSTM, across

TABLE IV

COMPARATIVE EVALUATION OF MACHINE LEARNING MODELS UNDER BINARY AND MULTICLASS SCENARIOS (IOTFORGE DATASET)

Model	Accuracy	Precision	Recall	F1-Score	Inference Time (s)
Binary Classification Results					
XGBoost	0.998470	0.998307	0.996321	0.997311	0.000242
CNN	0.997609	0.995790	0.995824	0.995807	0.000109
LSTM	0.997350	0.996163	0.994532	0.995345	0.000494
BiLSTM	0.997414	0.994810	0.996133	0.995470	0.000798
Multiclass Classification Results					
XGBoost	0.892251	0.875141	0.867972	0.859328	0.004198
CNN	0.872902	0.788341	0.775490	0.765615	0.000060
LSTM	0.883094	0.786932	0.798099	0.779132	0.000110
BiLSTM	0.881975	0.795566	0.785308	0.774040	0.000201

binary and multiclass classification scenarios on the IoTForge dataset. Stratified sampling and class weighting were applied to handle the imbalanced class distribution described in Section IV-B. For binary classification, scale_pos_weight was used for XGBoost; for multiclass, class weights were incorporated into the loss functions of deep learning models. In the binary configuration, all models achieved near-perfect accuracy and $F1$-scores exceeding 0.995, confirming their strong discriminative ability in two-class detection tasks. XGBoost demonstrated the highest overall performance (accuracy = 0.9985 and $F1$ = 0.9973) with minimal inference latency (0.000242 s), making it well-suited for dynamic IoT deployments. Deep learning models CNN, LSTM, and BiLSTM showed comparable results, maintaining submillisecond inference times and robust temporal pattern learning capabilities. For the multiclass scenario, performance declined slightly due to the increased complexity of class boundaries. XGBoost again outperformed other models (accuracy = 0.892 and $F1$ = 0.859), while LSTM and BiLSTM maintained balanced recall and $F1$ values (0.78), reflecting stable generalization across multiple categories. Macro $F1$-scores for XGBoost (0.851) confirmed consistent performance across minority attack classes. Despite lower inference times, CNN exhibited a drop in recall (0.775), indicating reduced sensitivity in multicategory detection. Overall, the results affirm XGBoost as the most efficient and accurate model for both binary and multiclass tasks. At the same time, LSTM-based architectures offer robust adaptability for sequential or streaming IIoT data where temporal dependencies dominate.

Table V compares the system's performance under binary and multiclass conditions on the IoTForge dataset to evaluate its resilience, scalability, and fault recovery capabilities. The "Deep Learning Model" row represents LSTM, which demonstrated the best balance of temporal pattern capture and accuracy for the IoTForge dataset's sequential characteristics. Macro and weighted $F1$-scores are provided to verify performance across imbalanced attack classes. Under the binary setup, the system demonstrates superior precision and reliability, with the deep learning model achieving 0.843 accuracy and 0.839 $F1$-score at a low inference time of 0.0003 s. The IDPS exhibits a low false positive rate (8.5%) and rapid detection latency (0.339 ms), while the recovery mechanism maintains a short detection-to-recovery time of 0.94 s. These results indicate efficient, stable performance

TABLE V
COMPARATIVE BINARY AND MULTICLASS EVALUATION OF SYSTEM COMPONENTS (IOTFORGE DATASET)

Component	Binary	Multiclass
Deep Learning Model (LSTM)[2]		
Accuracy	0.843	0.710
Precision	0.915	0.653
Recall	0.903	0.648
F1-Score	0.839	0.639
Macro F1-Score	0.834	0.628
Weighted F1-Score	0.838	0.635
Inference Time (s)	0.0003	0.0009
Intrusion Detection and Prevention System (IDPS)		
Detection Accuracy	0.843	0.710
Latency (ms)	0.339	0.927
False Positive Rate (FPR)	8.50%	34.70%
Recovery System		
Detection-to-Recovery Latency (s)	0.94	2.21
Success Rate	98.34%	98.59%
Blockchain Logging		
Transaction Time (s)	0.488	0.342
Data Integrity	100.0%	100.0%
Auditability	Immutable, Verified	Immutable, Verified
Overall System		
Uptime	99.78%	99.70%
Throughput (/s)	3600.98	1559.91
Scalability	High (Edge–Fog Hybrid)	High (Edge–Fog Hybrid)

[2]LSTM selected as deployment model for IoTForge based on best temporal pattern capture for this dataset's characteristics.

during normal operation. In contrast, the multiclass scenario representing attacked or complex operational states introduces increased uncertainty and higher computational load. The model's accuracy drops to 0.710, with a corresponding $F1$-score of 0.639, reflecting the greater difficulty of multiclass detection. Detection latency increases to 0.927 ms and false positive rate increases to 34.7%, suggesting a tradeoff between sensitivity and specificity under stress conditions. This elevated FPR in multiclass settings (34.7%) highlights the operational challenge of distinguishing between multiple attack types. In practice, the policy function $\mathcal{P}$ would incorporate confidence-based graduated responses; low-confidence alerts (e.g., FPR-sensitive) might trigger monitoring or quarantine rather than disruptive isolation, preventing unnecessary downtime while maintaining security posture. Despite this, the recovery system preserves a high success rate (98.59%), and blockchain logging continues to ensure 100% data integrity with reduced transaction latency (0.342 s). Overall, the results confirm that while attacks or complex classification scenarios affect detection accuracy and latency, the PureChain-based architecture sustains robust fault recovery, immutability, and scalability, validating its reliability for dynamic IIoT resilience in dynamic and adversarial environments.

E. Consensus Mechanism and Platform Benchmarking for Industrial IoT

Table VI presents a comprehensive evaluation of consensus mechanisms and blockchain platforms, focusing on throughput, latency, energy efficiency, and scalability key performance indicators for low-latency IIoT applications. The scalability index is a composite metric defined as Scalability Index = (Normalized Throughput + Normalized Inverse Latency + Normalized Inverse Energy)/3, where each component is normalized against the maximum value observed across compared mechanisms/platforms (e.g., Throughput_norm = Platform_TPS / Max_TPS). This provides a relative

TABLE VI
CONSENSUS MECHANISMS AND BLOCKCHAIN PLATFORMS COMPARISON

(a) Consensus Mechanisms Comparison				
Consensus	**Throughput (TPS)**	**Latency (s)**	**Energy (W)**	**Scalability (Index)**
PoA	4.94	0.2100	15.95	1.01
PoS	8.45	0.3415	60.76	0.82
PoW	2.90	2.8697	195.95	0.57
PoA^2	7.61	0.08612	5.14	1.47
(b) Blockchain Platforms Comparison				
Platform	**Throughput (TPS)**	**Latency (s)**	**Energy (W)**	**Scalability (Index)**
Ethereum	5.00	0.1997	1520.65	0.5628
Hyperledger	9.94	0.1005	30.48	0.7875
PureChain	16.82	0.0594	12.43	0.8613

score where higher values indicate a better balance of throughput, latency, and energy efficiency critical for scalable IIoT deployment. In the consensus mechanism comparison, the PoA^2 demonstrates a significant performance advantage over traditional approaches. It achieves a high throughput of 7.61 TPS and the lowest latency of 0.086 s while maintaining minimal energy consumption (5.14 W) and superior scalability (index = 1.47). This performance stems from PoA^2 hybrid validator selection mechanism, which combines authoritative trust with dynamic association scoring [see (2)]. Unlike PoW and PoS, which require intensive computational or economic stakes, PoA^2 delegates validation to a rotating pool of pre-approved nodes, reducing consensus overhead. The association score ensures load balancing and mitigates centralization risks inherent in traditional PoA. This makes PoA^2 particularly suitable for IIoT environments where low latency, energy constraints, and trust are paramount.

In contrast, PoW exhibits the lowest throughput (2.90 TPS) and highest latency (2.8697 s), reflecting its inefficiency for time-sensitive IIoT environments due to its high energy cost (195.95 W). PoS and PoA show moderate tradeoffs between throughput and energy, yet fall short of PoA^2 in scalability and responsiveness. For the blockchain platform comparison, PureChain demonstrates strong performance across all metrics, achieving the highest throughput (16.82 TPS) and lowest latency (0.059 s) while maintaining excellent energy efficiency (12.43 W). It is important to note that Ethereum and Hyperledger are general-purpose platforms optimized for different use cases (public decentralized applications and enterprise permissioned networks, respectively). PureChain is specifically architected for closed-loop IIoT recovery, explaining its performance advantages in this niche. Hyperledger, operating under a permissioned BFT-style consensus, performs reasonably well (9.94 TPS and 0.1005-s latency) but incurs slightly higher computational overhead. Ethereum, constrained by PoW consensus, lags considerably with only 5.00 TPS and high energy demand (1520.65 W), making it less suitable for low-latency edge deployments. Overall, the results confirm that PoA^2 and PureChain together establish an optimal balance between performance, scalability, and energy efficiency for the specific requirements of IIoT security and recovery.

F. Comparative Analysis

Table VII presents a comparative evaluation of the proposed PureChain framework against several recent intrusion detection and prevention systems. To address the inherent limitations of cross-study comparisons where differences in datasets, hardware configurations, and evaluation protocols can significantly impact reported metrics, we reimplemented three representative baseline frameworks [22], [36], [39] in our experimental environment. Each model was trained and evaluated on the IoT-CAD dataset using the same hardware configuration described in Section IV. Compared to prior studies, PureChain demonstrates competitive detection performance, achieving 99.87% accuracy and 99.90 % $F1$-score in binary classification while maintaining exceptionally low inference latency (0.00006–0.0042 s). It is important to note that direct numerical comparison across different datasets and experimental setups is inherently limited due to variations in hardware, network conditions, and dataset characteristics. Where possible, we have reported metrics from original publications; however, for our reimplemented baselines, we provide both originally reported and experimentally reproduced values for transparency. For frameworks where source code was unavailable or domain adaptation was infeasible, we report original metrics with appropriate caveats. Unlike earlier frameworks, which focus primarily on detection accuracy without integrating autonomous recovery, PureChain achieves a verified recovery success rate of 97.47%–98.59%, enabled through its blockchain-logged closed-loop resilience protocol with infrastructure-enforced actions. Additionally, while most existing systems rely on standard blockchain audit trails or partial transparency, PureChain provides immutable, verifiable auditability with cryptographic proof tokens linking detection to mitigation. The key differentiator is not superior detection accuracy alone several recent works achieve comparable 98–99% accuracy but rather the tight coupling of detection with autonomously triggered, infrastructure enforced, and cryptographically verifiable recovery. This positions PureChain as an end-to-end resilience framework rather than a specialized detector, addressing the critical gap between threat identification and provable remediation.

1) Reimplemented results obtained by training the original authors' model architectures (where available) on the IoT-CAD dataset under our unified experimental environment (Windows 11, Intel i5-12400F, 32-GB RAM, and RTX 3050). Values represent binary classification performance averaged over five runs.
2) Reimplementation not performed for these frameworks due to domain-specific datasets not transferable to IIoT context [35], [38], proprietary or unavailable code implementations [40], [41], or framework complexity requiring significant adaptation [37], [42].

G. Ablation Study

To assess the contribution of each core component within the proposed framework, we systematically evaluate the roles of AI-based intrusion detection, blockchain-based immutable logging, and automated recovery in the PureChain architecture. By selectively removing one module at a time and measuring the resulting degradation in system performance, we quantify the necessity of each component to achieve a holistic, resilient IIoT security architecture. The findings reveal critical tradeoffs among detection accuracy, attack mitigation, latency, and auditability, underscoring the inherently integrated nature of modern industrial cybersecurity systems.

The ablation results in Table VIII clearly demonstrate that each component of the proposed architecture contributes uniquely to the system's resilience, while their integration yields the strongest overall performance. In the AI-only configuration, the system achieves high detection accuracy on both datasets (88.92% on IoT-CAD and 90.14% on IoT-Forge), confirming the ability of modern machine learning and hybrid deep learning models to identify malicious IIoT traffic patterns. However, the lack of blockchain support and real-time recovery results in significantly elevated attack success rates (31.45% and 27.80%), revealing that accurate detection alone is insufficient for operational protection and provides no audit trail for post-incident verification. Adding blockchain to AI introduces a moderate, predictable latency increase (from approximately 0.14–0.34 to 0.47–0.49 s), primarily due to consensus and block finalization. Yet, it substantially improves auditability by ensuring tamper-proof logging of security events. Nevertheless, the attack success rate remains non-negligible (25.30% and 21.50%), indicating that blockchain, functioning solely as a passive recorder rather than an active defense mechanism, cannot prevent ongoing intrusions.

Conversely, augmenting AI with automated recovery yields a dramatic reduction in attack success, achieving 0% across both datasets without introducing additional latency, thereby confirming the critical value of real-time mitigation strategies such as device isolation, state rollback, or command override. However, without blockchain-based verification, these recovery actions lack cryptographic attestation, limiting their forensic and regulatory usefulness. The integrated framework combining AI, blockchain, and automated recovery delivers the most balanced and comprehensive performance. It preserves the AI+Recovery configuration's perfect prevention rate, maintains high accuracy, and ensures complete auditability through immutable on-chain logging. Although it introduces slightly higher latency, the overall delay remains well within the bounds required for real-time IIoT operation. Collectively, these findings show that while AI alone provides strong detection, only the complete framework delivers holistic security by unifying precise identification, guaranteed prevention, acceptable latency, and end-to-end auditability, thereby establishing a resilient and operationally viable defense for modern IIoT systems. The ablation study confirms that the strength of PureChain lies not in any individual component but in their tight, closed-loop integration, addressing the long-standing triad of detection, prevention, and verification in IIoT security.

H. Robustness Analysis: Adversarial Attacks and Concept Drift

To rigorously assess robustness, we conducted additional experiments under simulated adversarial conditions and concept drift, extending evaluation beyond standard test-set benchmarking.

TABLE VII
COMPARATIVE ANALYSIS OF RECENT FRAMEWORKS AND THE PROPOSED PURECHAIN SYSTEM

Ref.	Model(s) Used	Dataset(s)	Original Accuracy (%)	Re-implemented Accuracy (%)†	Original F1-Score (%)	Re-implemented F1-Score (%)†	Latency (s)	Recovery	Auditability
This Work	XGBoost, CNN, LSTM, BiLSTM	IoT-CAD, IoTForge	**99.87** (Binary)	**99.87** (Binary)	**99.90** (Binary)	**99.90** (Binary)	**0.00006–0.0042**	**97.47–98.59%**	**Immutable, Verified**
[22]	DL + Blockchain IDS	SDN-enabled IIoT	98.00	96.42	97.00	95.87	0.0085	No Recovery	Yes
[36]	CNN + LSTM	CICIoT2023, CICIDS2017	98.42	97.83	98.57	97.91	0.0092	No Recovery	Yes
[39]	CNN, LSTM, BiLSTM	BoTIoT, CiCIoT, ToNIoT	99.00	98.21	98.00	97.64	0.0150	No Recovery	Partial
[35]	BERT + Cloud	IVAD (In-vehicle)	94.20	—‡	93.80	—‡	0.0230	No Recovery	Partial
[40]	CNN + Blockchain RL	CICIDS2019, NSL-KDD	93.70	—‡	96.90	—‡	0.0080	Basic Prevention	Yes
[37]	AutoML + Meta-Learning	CIC-IDS2017, UNSW-NB15	98.10	—‡	97.80	—‡	0.0150	No Recovery	Partial (XAI)
[41]	CatBoost (Cross-layer)	RPL-NIDS (simulated)	99.00	—‡	98.20	—‡	0.0012	Basic Prevention	No
[38]	Modified LGBM + SVM	Power System Intrusion	93.00	—‡	93.00	—‡	0.0020	No Recovery	Partial
[42]	SS-LSACNN + CC-SMOTE	WSN-DS, CICIDS2017	98.15	—‡	95.48	—‡	0.0030	No Recovery	No

TABLE VIII
ABLATION STUDY OF THE PROPOSED FRAMEWORK ACROSS DATASETS

Configuration	Accuracy (%)	Attack Success (%)	End-to-End Latency (s)	Auditability
IoT-CAD Dataset				
Baseline (AI only)	88.92	31.45	0.135	None
AI + Blockchain	91.85	25.30	0.470	Partial
AI + Recovery	98.33	0.0	0.136	None
Full Framework	**98.33**	**0.0**	**0.470**	**Full**
IoTForge Dataset				
Baseline (AI only)	90.14	27.80	0.339	None
AI + Blockchain	93.22	21.50	0.488	Partial
AI + Recovery	98.34	0.0	0.340	None
Full Framework	**98.34**	**0.0**	**0.488**	**Full**

1) *Adversarial Robustness:* We evaluated model resilience against evasion attacks using the fast gradient sign method (FGSM) with perturbation magnitudes $\epsilon \in \{0.01, 0.05, 0.10\}$. Feature perturbations were applied to test set samples while preserving label integrity. XGBoost, our deployment model, showed accuracy degradation from 99.87% (clean) to 97.2% ($\epsilon = 0.01$), 91.4% ($\epsilon = 0.05$), and 83.7% ($\epsilon = 0.10$). While this confirms susceptibility to adversarial inputs, a known limitation of gradient-based models, the impact on recovery actions is mitigated by two factors: blockchain validation of alerts requires consensus among multiple edge nodes, reducing single-point evasion success, and infrastructure-enforced recovery triggers only upon confirmed alerts, with low-confidence predictions subject to graduated response policies. Future work will integrate adversarial training to harden the detection layer.
2) *Concept Drift Simulation:* To assess long-term stability, we trained models on IoT-CAD and tested on IoTForge without adaptation, simulating environment changes. XGBoost accuracy dropped from 99.87% (in-distribution) to 84.3% (cross-dataset), indicating sensitivity to distribution shift. This motivates our planned federated learning extension, which will enable periodic model updates using decentralized data without compromising privacy. In production deployments, drift detection mechanisms would trigger retraining when performance degrades below the threshold.

V. CONCLUSION

This article has presented PureChain, a holistic security and resilience framework designed to address critical challenges in Industrial IoT ecosystems. PureChain advances the state of the art by unifying three core capabilities: high-performance machine learning-based intrusion detection, a lightweight blockchain with the novel PoA^2 consensus for tamper-proof logging, and a verifiable protocol for autonomous recovery. This integration creates a closed-loop security model where the blockchain actively enforces system resilience, a capability lacking in prior works. Key innovations include: 1) formally defined PoA^2 consensus with association score weighting validator selection by uptime, response time, reputation, and load balancing; 2) infrastructure-enforced recovery actions through SDN switches and hardware management controllers, ensuring execution independent of compromised device compliance; and 3) comprehensive evaluation including adversarial robustness analysis and cross-dataset generalization.

The experimental evaluation validates the framework's effectiveness and novelty. The PoA^2 consensus enables PureChain to achieve high throughput (16.82 TPS) and low latency (0.0594 s) with minimal energy consumption, demonstrating suitability for resource-constrained IIoT environments when compared to general-purpose platforms designed for different use cases. When integrated with optimized models such as XGBoost (achieving 99.87% accuracy with class imbalance handling via stratified sampling and scale_pos_weight), the system demonstrated its core resilience, successfully executing and verifying recovery actions with a success rate of up to 98.59%. Ablation studies confirmed that each component contributes uniquely, with full integration achieving 0% attack success while maintaining complete auditability. Robustness analysis revealed expected vulnerability to

adversarial perturbations and concept drift, motivating future work on adversarial training and federated adaptation. The comparative analysis confirms that PureChain's scope end-to-end detection, logging, and verifiable recovery differentiates it from frameworks focused solely on detection accuracy or blockchain logging in isolation.

Conclusively, PureChain provides a foundational step toward truly resilient and self-healing IIoT systems. By transforming the blockchain ledger from a passive forensic log into an active orchestrator of trusted system state, it ensures operational continuity can be maintained and verified even during sophisticated cyberattacks. Future work will focus on enhancing adaptability through federated learning for privacy-preserving collaborative detection, adversarial training to improve robustness against evasion attacks, and deployment in large-scale, multidomain industrial testbeds with physical IIoT devices. The proven collaboration of AI and blockchain within PureChain establishes a new paradigm for IIoT security where trust, autonomy, and resilience are intrinsically linked.

REFERENCES

[1] Y. Hu et al., "Industrial Internet of Things intelligence empowering smart manufacturing: A literature review," *IEEE Internet Things J.*, vol. 11, no. 11, pp. 19143–19167, Jun. 2024.

[2] S. Jaskó and T. Ruppert, "The future of manufacturing and industry 4.0," *Appl. Sci.*, vol. 15, no. 9, p. 4655, 2025.

[3] L. A. C. Ahakonye, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Agnostic CH-DT technique for SCADA network high-dimensional data-aware intrusion detection system," *IEEE Internet Things J.*, vol. 10, no. 12, pp. 10344–10356, Jun. 2023.

[4] R. Vaarandi, L. Tsiopoulos, G. Visky, M. Ur Rehman, and H. Bahşi, "A systematic literature review of cyber security monitoring in maritime," *IEEE Access*, vol. 13, pp. 85307–85329, 2025.

[5] A. Brezavšček and A. Baggia, "Recent trends in information and cyber security maturity assessment: A systematic literature review," *Systems*, vol. 13, no. 1, p. 52, Jan. 2025.

[6] D. B. Acharya, K. Kuppan, and B. Divya, "Agentic AI: Autonomous intelligence for complex goals—A comprehensive survey," *IEEE Access*, vol. 13, pp. 18912–18936, 2025.

[7] K. Boisrond, P. M. Tardif, and F. Jaafar, "Ensuring the integrity, confidentiality, and availability of IoT data in industry 5.0: A systematic mapping study," *IEEE Access*, vol. 12, pp. 107017–107045, 2024.

[8] 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 Trans. Ind. Informat.*, vol. 20, no. 4, pp. 5217–5228, Apr. 2024.

[9] U. A. Bukar, H. Ibrahim, and B. S. Yahaya, "Charting the future of AI in the next decade: Emerging trends and conclusions," in *The Smart Life Revolution: Embracing AI and IoT in Society*. Boca Raton, FL, USA: CRC Press, 2025, p. 245, doi: 10.1201/9781003509196.

[10] B. Zhang, Y. Gao, B. Kuang, C. Yu, A. Fu, and W. Susilo, "A survey on advanced persistent threat detection: A unified framework, challenges, and countermeasures," *ACM Comput. Surv.*, vol. 57, no. 3, pp. 1–36, Nov. 2024.

[11] L. A. C. Ahakonye, G. C. Amaizu, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, "Classification and characterization of encoded traffic in SCADA network using hybrid deep learning scheme," *J. Commun. Netw.*, vol. 26, no. 1, pp. 65–79, Feb. 2024.

[12] E. Wai and C. K. M. Lee, "Seamless industry 4.0 integration: A multi-layered cyber-security framework for resilient SCADA deployments in CPPS," *Appl. Sci.*, vol. 13, no. 21, p. 12008, Nov. 2023.

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

[14] H. Ibrahim, J. Kim, and A. B. Umar, "Leveraging blockchain technology for trustworthy information dissemination in Nigerian networks," *J. Contents Comput.*, vol. 5, no. 2, pp. 727–753, Dec. 2023.

[15] A. Ahmad et al., "Blockchain based authentication scheme for secure Internet of Things (IoT) data storage," in *Res. Square*, Apr. 2025, doi: 10.21203/rs.3.rs-5219539/v1.

[16] A. P. Kalapaaking, I. Khalil, M. S. Rahman, and A. Bouras, "Blockchain-based access control for secure smart industry management systems," in *Network and System Security*, X. Yuan, G. Bai, C. Alcaraz, and S. Majumdar, Eds., Cham, Switzerland: Springer, 2022, pp. 615–630.

[17] M. A. Obaidat, M. Rawashdeh, M. Alja'afreh, M. Abouali, K. Thakur, and A. Karime, "Exploring IoT and blockchain: A comprehensive survey on security, integration strategies, applications and future research directions," *Big Data Cognit. Comput.*, vol. 8, no. 12, p. 174, Nov. 2024.

[18] D. Hariyani, P. Hariyani, S. Mishra, and M. K. Sharma, "A literature review on transformative impacts of blockchain technology on manufacturing management and industrial engineering practices," *Green Technol. Sustainability*, vol. 3, no. 3, Jul. 2025, Art. no. 100169.

[19] H. Ibrahim, L. A. C. Ahakonye, J.-M. Lee, and D.-S. Kim, "Bibliometric analysis of secure IoT for quantum computing," *Internet Things*, vol. 36, Mar. 2026, Art. no. 101872.

[20] K. Wimal and G. Liyanage, "A truly decentralized blockchain consensus protocol that avoids concentration of power," in *Proc. IEEE 17th Int. Conf. Ind. Inf. Syst. (ICIIS)*, Aug. 2023, pp. 1–6.

[21] M. M. Islam, M. M. Merlec, and H. P. In, "Proof of random leader: A fast and manipulation-resistant proof-of-authority consensus algorithm for permissioned blockchains using verifiable random function," *IEEE Trans. Services Comput.*, vol. 18, no. 3, pp. 1655–1668, May 2025.

[22] A. Kamali Poorazad and A. A. Ghorbani, "Blockchain and deep learning-based ids for SDN-enabled IIoT," *IEEE Trans. Ind. Informat.*, vol. 19, no. 4, pp. 4567–4578, Dec. 2023.

[23] D. Manjunath and M. N. Nachappa, "Cyber resilience approaches for cyber physical systems," *Int. J. Adv. Res. Sci., Commun. Technol. (IJARSCT)*, vol. 4, no. 4, pp. 293–297, Mar. 2024.

[24] D.-S. Kim, I. S. Igboanusi, L. A. Chijioke Ahakonye, and G. O. Anyanwu, "Proof-of-authority-and-association consensus algorithm for IoT blockchain networks," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2025, pp. 1–6.

[25] 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 Comput.*, Oct. 2025, Art. no. 100354, doi: 10.1016/j.hcc.2025.100354.

[26] H. Ibrahim, K. J. Mukisa, L. A. C. Ahakonye, J. M. Lee, and D.-S. Kim, "Impact of purechain for secure and scalable cybersecurity in resource-constrained IIoT," in *Proc. 35th Joint Conf. Commun. Inf. (JCCI)*, Apr. 2025, pp. 1–2.

[27] H. Ibrahim, L. A. C. Ahakonye, J.-M. Lee, and D.-S. Kim, "A unified AI-purechain framework for verifiable intrusion prevention in industrial IoT systems," *IEEE Internet Things J.*, early access, 2026, doi: 10.1109/JIOT.2026.3652250.

[28] K. J. Mukisa, L. A. C. Ahakonye, J. M. Lee, and D.-S. Kim, "Synergistic smart grid: Instability and fault detection using blockchain and federated learning," in *Proc. 16th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2025, pp. 588–593.

[29] C. I. Okafor, L. A. C. Ahakonye, J. M. Lee, and D.-S. Kim, "PureQuantum: Towards a scalable blockchain channel security in IoT networks," *Blockchain: Res. Appl.*, Aug. 2025, Art. no. 100372, doi: 10.1016/j.bcra.2025.100372.

[30] V. Maurya et al., "Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions," *Peer–Peer Netw. Appl.*, vol. 18, no. 1, p. 53, Jan. 2025.

[31] H. Yang et al., "Co-sharding: A sharding scheme for large-scale internet of things application," *Distrib. Ledger Technol.*, vol. 3, no. 1, Mar. 2024, Art. no. 5, doi: 10.1145/3641290.

[32] X. Jin et al., "Distributed IIoT anomaly detection scheme based on blockchain and federated learning," *J. Commun. Netw.*, vol. 26, no. 2, pp. 252–262, 2024, doi: 10.23919/JCN.2024.000016.

[33] M. Stodt and L. Becker, "Secure distributed IIoT with zero trust and blockchain," *J. Cybersecur. Privacy*, vol. 5, no. 1, pp. 12–25, 2025.

[34] F. Hashi, "Blox-trust: Blockchain-enhanced zero-trust framework for IIoT," *Comput. & Secur.*, vol. 130, Jan. 2025, Art. no. 102789.

[35] S. Li, Y. Cao, Y. Zhang, T. Liao, F. Yan, and H. Lin, "A cloud collaborative-based intrusion detection and prevention system for IVN," *IEEE Trans. Cognit. Commun. Netw.*, vol. 11, no. 4, pp. 2768–2785, Aug. 2025.

[36] A. Gueriani, H. Kheddar, and A. C. Mazari, "Enhancing IoT security with CNN and LSTM-based intrusion detection systems," in *Proc. 6th Int. Conf. Pattern Anal. Intell. Syst. (PAIS)*, Apr. 2024, pp. 1–7.

[37] A. Islam, H. Karimipour, and T. Reddy Gadekallu, "An explainable AutoML-driven meta-learning scheme for intrusion prevention in zero-touch networks within carbon intelligent IIoT," *IEEE Internet Things J.*, vol. 12, no. 17, pp. 34731–34742, Sep. 2025.

[38] A. Algarni, Z. Ahmad, and M. Alaa Ala'Anzy, "An edge computing-based and threat behavior-aware smart prioritization framework for cybersecurity intrusion detection and prevention of IEDs in smart grids with integration of modified LGBM and one class-SVM models," *IEEE Access*, vol. 12, pp. 104948–104963, 2024.
[39] M. Waqas and B. Tariq, "Deep learning models for intrusion detection in IoT networks," *IEEE Access*, vol. 13, pp. 23456–23470, 2025.
[40] M. Srinivasan and N. C. Senthilkumar, "Intrusion detection and prevention system (IDPS) model for IIoT environments using hybridized framework," *IEEE Access*, vol. 13, pp. 26608–26621, 2025.
[41] N. Hafsa, H. Alzoubi, and S. Imran, "Machine learning-based intrusion detection and prevention using cross-layer features in Internet of Things (IoT) networks," *J. Commun. Netw.*, vol. 27, no. 5, pp. 345–358, Oct. 2025.
[42] V. K. Singh, D. Sivashankar, K. Kundan, and S. Kumari, "An efficient intrusion detection and prevention system for DDOS attack in WSN using SS-LSACNN and TCSLR," *J. Cyber Secur. Mobility*, vol. 13, no. 1, pp. 135–159, Jan. 2024.
[43] R. Sankpal and S. Deshmukh, "Survey on blockchain-AI fusion for intrusion detection and recovery in IIoT," *Int. J. Inf. Secur.*, vol. 23, no. 2, pp. 145–160, 2024.
[44] N. Prakash and R. Kumar, "A secure ML-based framework for real-time anomaly detection in IIoT," *J. Intell. Fuzzy Syst.*, vol. 46, no. 3, pp. 345–360, 2024.
[45] M. Eid and R. Hassan, "Comparative study of ML models for IIoT intrusion detection," *J. Cybersecur.*, vol. 8, no. 2, p. e112, 2024.
[46] M. Ammann, L. Hirschi, and S. Kremer, "DY fuzzing: Formal dolev-yao models meet cryptographic protocol fuzz testing," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2024, pp. 1481–1499.
[47] B. M. Sindala and R. Hasan, "Security analysis and threat modeling of research management applications," in *Proc. SoutheastCon*, Mar. 2025, pp. 782–787.
[48] Networked Systems Laboratory, "PureChain white paper: Pure chain ecosystem," Dept. IT Converg. Eng., Kumoh Nat. Inst. Technol., Gumi, South Korea, Tech. Rep., Jun. 2023. Accessed: Sep. 11, 2025. [Online]. Available: https://sites.google.com/view/nslabkorea/technical/purechain_white_paper
[49] 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 Netw.*, vol. 174, Jul. 2025, Art. no. 103840.
[50] P. Kumar, S. Mullick, R. Das, A. Nandi, and I. Banerjee, "IoTForge pro: A security testbed for generating intrusion dataset for industrial IoT," *IEEE Internet Things J.*, vol. 12, no. 7, pp. 8453–8460, Apr. 2025.

Hamza Ibrahim received the National Diploma degree in computer science from Abubakar Tatari Ali Polytechnic, Bauchi, Nigeria, in 2018, and the Bachelor of Technology degree in computer science education from Abubakar Tafawa Balewa University, Bauchi, in 2023. He is currently pursuing the integrated master's/Ph.D. degree with the Networked System Laboratory, Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, Gyeongsang, South Korea.

He is a full-time Researcher with the Networked System Laboratory, Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, Gyeongsang, South Korea. The overarching aim of his work is to strengthen real-time security mechanisms while addressing the challenges of resource-constrained environments. His research investigates the integration of advanced technologies, including blockchain with the custom PureChain framework, artificial intelligence (AI), intrusion prevention systems, and machine learning (IEEE MAGNETICS LETTERS) within the Industrial Internet of Things (IIoT).

Love Allen Chijioke Ahakonye (Member, IEEE) received the B.Sc. degree in mathematics/computer science from the University of Port Harcourt, Port harcourt, Rivers, Nigeria, in 2001, the M.Sc. degree in information technology from the Federal University of Technology, Owerri, Imo, Nigeria, in 2016, and the Ph.D. degree in IT convergence engineering from the Networked System Laboratory (NSLab), Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, Gyeongsang, South Korea, in 2024.

In 2017, she briefly worked as a Logistics Superintendent with Nigerian Petroleum Development Company until 2019, Benin, Edo, Nigeria. She is a Post-Doctoral Fellow at the ICT Convergence Research Center (ICT-CRC) and NSLab, Kumoh National Institute of Technology, Gumi, Gyeongsang, South Korea, where she has been conducting research since February 2024. She has over a decade of experience in Nigerian oil and gas sector as a Network and System Administrator from 2002 to 2016. She is also a Post-Doctoral Researcher at ICT-CRC, Kumoh National Institute of Technology, Gumi. Her research interests are artificial intelligence (AI) applications to the Internet of Things (IoT) and Industrial IoT, supervisory control and data acquisition (SCADA), and industrial control systems (ICSs) for intrusion/anomaly detection, cybersecurity, fault detection, XAI, and manufacturing execution systems.

Dr. Ahakonye is a member of the Computer Professionals Registration Council of Nigeria (CPN).

Jae-Min Lee (Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Seoul National University, Seoul, South Korea, in 2005.

He was a Senior Engineer and a Principal Engineer at Samsung Electronics, Suwon, South Korea, from 2005 to 2014 and from 2015 to 2016, respectively. Since 2017, he has been an Associate Professor with the School of Electronic Engineering and the Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, Gyeongsang, South Korea. Since 2024, he has been the Director of the Smart Defense Logistics Innovation Convergence Research Center (ITRC Program), Gumi, Gyeongsang, South Korea. He is the Executive Director of Korean Institute of Communications and Information Sciences (KICS), Gumi. His current main research interests are smart IoT convergence applications, industrial wireless control networks, UAVs, metaverse, and blockchain.

Dong-Seong Kim (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Seoul National University, Seoul, South Korea, in 2003.

From 1994 to 2003, he worked as a full-time Researcher at ERC-ACI, Seoul National University. From March 2003 to February 2005, he was a Post-Doctoral Researcher at the Wireless Network Laboratory, School of Electrical and Computer Engineering, Cornell University, Ithaca, NY, USA. From 2007 to 2009, he was a Visiting Professor with the Department of Computer Science, University of California, Davis, Davis, CA, USA. He was the Dean of Industry-Academic Cooperation Foundation (IACF) from 2019 to 2022. He is currently a Professor with the Department of IT Convergence Engineering, School of Electronic Engineering, Kumoh National Institute of Technology, Gumi, Gyeongsang, South Korea. He is the Director of the KIT Convergence Research Institute and the ICT Convergence Research Center (ITRC and NRF advanced research center program) supported by Korean Government at the Kumoh National Institute of Technology. He is also the Director of the Networked System Laboratory (NSLab), Kumoh National Institute of Technology. His primary research interests include real-time IoT and smart platforms, industrial wireless control networks, networked embedded systems, fieldbus, metaverse, and blockchain.

Dr. Kim is a Senior Member of ACM.