A Unified AI-PureChain Framework for Verifiable Intrusion Prevention in Industrial IoT Systems

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

***Abstract*—Securing industrial Internet of Things (IIoT) systems presents critical challenges due to resource constraints, expanding attack surfaces, and the inadequacy of conventional security solutions against sophisticated cyber threats. While AI-driven detection and blockchain technologies offer promise, existing frameworks suffer from computational inefficiency, a lack of real-time prevention, or insufficient auditability. This article introduces a unified AI-PureChain intrusion prevention framework that tightly integrates deep learning-based threat detection with an immutable PureChain ledger using proof of authority and association (PoA^2) consensus. The proposed architecture achieves high-fidelity intrusion detection through hybrid CNN-BiLSTM models, attaining 99.76% accuracy on IoTForge Pro, 98.33% on WUSTL-IIoT-2021, and 98.11% on X-IIoTID datasets, while maintaining low inference latency (0.0016 s). The PureChain layer ensures tamper-proof audit trails with 24.56 transactions per second (TPS) throughput and 68-ms commit time, enabling verifiable prevention actions. Experimental results demonstrate complete attack mitigation (0% success rate) under high-traffic conditions while maintaining minimal resource consumption (14.49% CPU, 448-MB memory, 12.95-W power). This work represents a significant advancement in IIoT security by delivering a tightly coupled framework that simultaneously addresses detection accuracy, prevention reliability, and forensic accountability, thereby bridging critical gaps in current industrial security paradigms.**

***Index Terms*—Blockchain, cyber-physical systems, industrial IoT security, intrusion prevention system (IPS), PureChain.**

I. Introduction

SECURING industrial Internet of Things (IIoT) systems remains a persistent challenge due to their resource limitations and increasing exposure to sophisticated cyber threats [1], [2]. While IIoT technologies interconnect sensors, actuators, and control systems to enhance productivity and enable data-driven automation [3], [4], [5], this convergence of operational technology (OT) and information technology (IT) has significantly expanded the attack surface [6]. Industrial environments are now increasingly vulnerable to attacks such as unauthorized access, data tampering, and advanced persistent threats (APTs) [7], [8]. Unlike conventional IT systems, IIoT deployments rely heavily on constrained edge devices with limited computing, memory, and power resources [9]. These constraints hinder the deployment of conventional enterprise security solutions and highlight the need for lightweight, decentralized, and resilient protection frameworks [10]. Weak authentication, insecure telemetry, and minimal encryption further amplify vulnerabilities [11], [12]. IIoT security, therefore, demands adaptive and low-overhead mechanisms capable of preserving data integrity, ensuring real-time responsiveness, and maintaining operational continuity [2], [8].

Traditional perimeter defenses such as virtual local area network (VLAN) segmentation, firewalls, and network isolation provide limited protection in hyper-connected IIoT environments [3]. The modern IIoT ecosystem faces increasingly sophisticated and cross-layered threats that exploit architectural vulnerabilities. Ransomware and command injection attacks can disrupt production lines and inflict physical damage [13]. Large-scale distributed denial of service (DDoS) attacks and data integrity attacks target essential public infrastructures, causing operational paralysis [13]. In healthcare and cyber-physical domains, ransomware and medical device hijacking directly endanger patient safety [14]. Vehicular networks remain exposed to vehicle-to-everything (V2X) message spoofing and sensor manipulation, creating potential safety hazards [14]. Furthermore, man-in-the-middle (MitM) and Sybil attacks compromise the trust and reliability of decentralized machine-to-machine communications [15]. Collectively, these attack vectors reveal the critical security vulnerabilities spanning the cloud, communication, and edge layers of the IIoT ecosystem, as depicted in the integrated threat model (Fig. 1).

Once adversaries bypass these layers, lateral movement and protocol-specific vulnerabilities allow rapid compromise [7], [16]. This shortfall has driven research toward intrusion detection and prevention systems (IDPSs) that combine signature-based and anomaly-based techniques [16], [17]. While signature-based models fail against zero-day threats,

Received 19 December 2025; accepted 5 January 2026. Date of publication 12 January 2026; date of current version 26 March 2026. This work was supported in part by the Innovative Human Resource Development for Local Intellectualization program through the Institute for Information and Communications Technology Planning and Evaluation (IITP) grant funded by the Korea government Ministry of Science and ICT (MSIT) (25%) under Grant IITP-2026-RS-2020-II201612, in part by the Priority Research Centers Program through the NRF funded by the Ministry of Education, Science and Technology (MEST) (25%) under Grant 2018R1A6A1A03024003, in part by the MSIT, Korea, under the Information Technology Research Center (ITRC) support program (25%) under Grant IITP-2026-RS-2024-00438430, and in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (25%) under Grant RS-2025-25431637. *(Corresponding author: Dong-Seong Kim.)*

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

Digital Object Identifier 10.1109/JIOT.2026.3652250

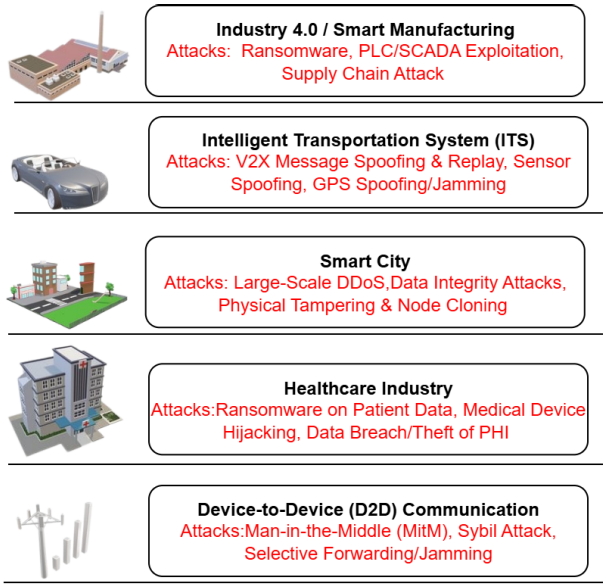

Fig. 1. Possible attacks across different domains of the IIoT environments.

anomaly-based methods suffer from high false positives and lack explainability [18]. Moreover, existing intrusion prevention systems (IPSs) frameworks rarely provide immutable auditing or forensic traceability, both of which are critical for industrial compliance and accountability [19], [20]. Blockchain technologies offer a strong foundation for building tamper-evident, transparent, and verifiable IIoT security frameworks [7], [21]. Their distributed nature ensures trusted data provenance and auditability. Yet, mainstream consensus algorithms such as proof-of-work (PoW) and proof-of-stake (PoS) remain computationally expensive, while proof-of-authority (PoA) introduces risks of validator centralization [22], [23]. Platforms like Ethereum and Hyperledger Fabric also incur high latency and significant resource costs, reducing their suitability for constrained IIoT deployments [24].

To overcome these limitations, research has advanced lightweight blockchain designs optimized for low-latency, energy efficiency, and IoT scalability [8], [11]. Parallel efforts have also explored AI-based IPS solutions for adaptive, real-time detection [16], [17]. The convergence of these two directions, AI-driven prevention and blockchain-based accountability, creates an opportunity to build proactive, trustworthy IIoT defense frameworks [25]. Among emerging blockchain architectures, PureChain is a custom blockchain explicitly designed for IoT environments, employing the proof of authority and association (PoA^2) consensus mechanism [26], [27]. Unlike conventional blockchains, PureChain operates at the transaction layer to eliminate block delays and ensure deterministic finality through trusted validator nodes, effectively resolving the blockchain "quad-lemma" of decentralization, security, scalability, and cost [28], [29]. Evaluations in [30] reveal that PureChain improves throughput by 230%, reduces latency by 70%, and enhances scalability over Ethereum and Hyperledger. This makes it well-suited for real-time industrial operations that demand both speed and verifiable integrity.

Despite these advancements, current literature reveals significant gaps: 1) most AI-based detection systems operate in isolation without real-time prevention capabilities; 2) blockchain implementations remain passive backends lacking integration with security response mechanisms; and 3) existing frameworks fail to provide the tight coupling required for verifiable, real-time intrusion prevention in resource-constrained IIoT environments. Thus, in this study, we introduce a unified AI-PureChain intrusion prevention framework that tightly couples deep learning-based detection with blockchain-backed verification. The system enables decentralized, privacy-preserving, and auditable intrusion prevention for IIoT environments, achieving both real-time responsiveness and forensic accountability. The main contributions are as follows.

1) A high-fidelity AI detection mechanism using hybrid CNN-BiLSTM models that accurately identifies and classifies cyber threats in real-time with 99.76% accuracy and 0.0016-s inference latency.
2) A novel integration of PureChain's PoA^2 consensus with AI detection, creating an immutable ledger for tamper-proof security event logging with 24.56 transactions per second (TPS) throughput and 68-ms commit time optimized for IPS operations.
3) A proactive IPS response system that executes deterministic mitigation actions (quarantine, throttle, allow) with immediate PureChain auditability, ensuring accountability and traceability.
4) A comprehensive experimental evaluation across three benchmark datasets demonstrating the framework's effectiveness in achieving 0% attack success rate under high traffic while maintaining low resource consumption (14.49% CPU, 448-MB memory).

To the best of our knowledge, this is the first work that successfully integrates AI-driven detection, PureChain blockchain auditability, and proactive IPS response into a unified architecture specifically designed for the stringent operational constraints of Industrial IoT networks.

The rest of the article is structured as follows. Section II provides a critical review of the literature on IIoT security frameworks, building upon the introduction in Section I. Section III details the architecture of the proposed solution. Section IV presents the experimental setup, comprehensive performance evaluation, and comparative analysis with state-of-the-art approaches. Finally, Section V concludes the article and suggests promising avenues for future research.

II. Background and Related Work

The security of IIoT networks requires solutions that are not only intelligent, but also resilient, auditable, and automated [31], [32]. Existing research spans several key areas: AI-driven detection, blockchain-based security, integrated systems, and classical IPS. This section critically analyzes the state-of-the-art, explicitly highlighting the advances and limitations that motivate our proposed framework. We structure our review to emphasize the research gaps and position our contributions relative to recent work from top venues in IoT security and blockchain research.

A. AI and Machine Learning for IIoT Intrusion Detection

A significant body of recent work focuses on using machine learning to identify threats in IIoT network traffic. Researchers have primarily pursued improvements in detection accuracy and computational efficiency. Jan et al. [33] developed a hybrid CNN-LSTM model that effectively captures spatial and temporal features in traffic flows. Similarly, Alsaedi et al. [34] proposed an unsupervised deep belief network (DBN) model to address the challenge of limited labeled data. Zhang et al. [35] introduced a graph neural network (GNN) approach to model complex relationships between IIoT devices, showing improved detection of coordinated attacks.

Efforts to improve efficiency are equally prominent. Fatima et al. [36] proposed a lightweight IDS utilizing a refined decision tree algorithm to minimize computational overhead, demonstrating the practicality of resource-aware solutions. Mahmud et al. [37] developed a federated learning framework in which local models are trained directly on edge devices, preserving data privacy. From an adversarial perspective, Vitorino et al. [38] examined the susceptibility of deep learning-based IDS to evasion attacks, highlighting the challenges of maintaining robustness. While these studies advance detection capabilities, they largely treat AI as an isolated component, offering limited insight into its integration with real-time prevention and immutable logging. Moreover, recent works such as Chen et al. [17], and Esmaeili et al. [18] continue to focus on detection accuracy without addressing the need for verifiable prevention mechanisms; an architectural gap our framework addresses.

B. Blockchain for Security and Auditability in IIoT

Blockchain technology is recognized for its potential to introduce trust, transparency, and nonrepudiation into IIoT systems. Research in this area often focuses on consensus mechanisms and scalable data structures. Mahajan and Reddy [39] proposed a lightweight blockchain framework for data provenance using PBFT, while Abbasi et al. [40] explored DPoS to enhance throughput and efficiency in IIoT data auditing. Jayabalan and Jeyanthi [41] addressed storage concerns through off-chain IPFS channels for healthcare data. However, mainstream blockchain platforms face significant limitations in scalability, latency, and energy consumption, making them unsuitable for high-frequency IoT applications [42]. These studies, including Arshad et al. [43] on access control and Yohan et al. [44] on firmware updates, primarily treat blockchain as a passive backend. They do not meet the real-time, low-latency demands of dynamic IIoT environments. This gap underscores the need for blockchain frameworks purpose-built for operational security. PureChain addresses this by employing the PoA^2 consensus mechanism at the transaction layer to eliminate block delays and ensure deterministic finality through trusted nodes, effectively resolving the blockchain "quadlemma" of decentralization, security, scalability, and cost [26], [27], [28].

C. Integrated AI–Blockchain Architectures

The convergence of AI and blockchain is an emerging research direction, though most implementations remain loosely coupled. Mondal and Roy [45] surveyed sequential approaches where ML detects threats and blockchain stores data. Mansour [46] proposed BAC-IDS, integrating clustering and blockchain for secure transmission. Akrasi-Mensah et al. [47] applied deep reinforcement learning to optimize blockchain scalability, while Ali et al. [48] introduced TrustShare for secure threat intelligence sharing. Recent efforts embed blockchain more deeply into security-critical IoT environments. Okafor et al. [49] integrated QKD into PoA^2 consensus for validator security, and Nakayiza et al. [50] developed a blockchain-enhanced IDS for vehicular networks. While promising, these works remain domain-specific and lack a generalizable, tightly integrated architecture for real-time intrusion prevention. They typically employ sequential processing (detect-then-log) rather than the integrated feedback loop we propose, precisely the gap our framework aims to fill.

D. IPSs for IIoT

Research on IPSs forms a foundational layer in IIoT security. Classical signature-based IPSs, reviewed by Kumar et al. [51], offer low false-positive rates but fail against zero-day threats. Adaptive approaches have emerged: Mishra et al. [52] explored SDN-based IPS for dynamic reconfiguration, and Afrin et al. [53] emphasized policy-driven automated responses. Recent advancements in adaptive IPS include the work of Sajid et al. [16] on hybrid machine learning approaches, and Chen et al. [17] on two-stage classifiers. However, current systems lack immutable records of mitigation actions and verifiable audit trails, posing operational risks in industrial settings where accountability and traceability are essential.

E. Summary and Research Gap

While AI-based detection, blockchain-enabled auditability, and IPS automation have each advanced independently, existing solutions fall short of delivering a unified, real-time, and verifiable security framework tailored for IIoT. Table I summarizes the limitations of current approaches and highlights our contributions. Most approaches treat these components in isolation or with loose coupling, failing to meet the stringent demands of industrial environments. Key research gaps include: 1) lack of tight integration between AI detection and blockchain auditability; 2) absence of real-time prevention with verifiable audit trails; and 3) insufficient attention to resource efficiency in combined AI-blockchain-IPS systems. Our proposed framework addresses this gap by tightly integrating AI-driven intrusion detection, PureChain PoA^2 blockchain for immutable logging, and proactive IPS response into a cohesive architecture purpose-built for IIoT resilience, scalability, and trust.

III. System Model

The proposed framework adopts a multilayered architecture to address the core challenges of modern IIoT security (see

TABLE I
COMPARATIVE SUMMARY OF EXISTING WORKS AND BENCHMARK AGAINST PROPOSED FRAMEWORK

Ref.	Approach	Strengths	Limitations	Proposed Framework Contribution
		AI for IIoT Intrusion Detection Systems (IDS)		
[34]	(CNN-LSTM)	Captures spatial temporal dependencies	No real-time prevention or audit integration	Integrates detection with blockchain-based audit and IPS
[35]	(DBN)	Unsupervised learning for limited labels	Lacks end-to-end integration	Provides real-time response with blockchain audit trail
[36]	(GNN)	Models device relations, coordinated attacks	High complexity, no live mitigation	Enables on-chain response and mitigation
[37]	(Decision Tree)	Lightweight, suitable for edge deployment	Limited detection depth	Balances efficiency and detection accuracy
[38]	(Federated Learning)	Privacy-preserving distributed training	No verifiable audit or trust layer	Integrates federated auditing via PureChain ledger
[39]	(Adversarial Robustness)	Addresses adversarial risks in IDS	No proactive defense mechanism	Adds self-healing and blockchain-logged IPS
		Blockchain for IIoT Security and Logging		
[40]	(PBFT)	Lightweight consensus for provenance	Backend-only, no live audit	Real-time PoA^2-based event recording
[41]	(DPoS)	High throughput for data trading	Passive data storage only	Enables on-chain accountability for each detection
[42]	(IPFS)	Scalable off-chain storage	Inefficient for live IIoT events	Real-time on-chain logging via validator consensus
[44]	(Access Control)	Decentralized trust management	No autonomous response capability	Adds blockchain-driven automated mitigation
[45]	(Firmware Updates)	Secure firmware validation	Domain-specific, limited generality	Generalizable for broader IIoT intrusion detection
		AI–Blockchain Integrated Frameworks		
[46]	(ML + Blockchain)	Combines ML with immutable storage	Loosely coupled sequential design	Fully integrated feedback-driven pipeline
[47]	(BAC-IDS)	Clustering and blockchain transmission	Fragmented architecture	Unified detection, logging, and adaptive control
[48]	(DRL)	Adaptive block selection	Focused on blockchain optimization	Balances detection, auditing, and control
[49]	(TrustShare)	Secure threat intelligence sharing	No live IPS or detection link	Real-time AI-driven detection and sharing
[50]	(PureQuantum)	QKD-enhanced PoA^2 validator security	Domain-limited (IoT)	Extends PoA^2 to IIoT anomaly logging
[51]	(PureChain-IDS for IoV)	Lightweight AI with blockchain logging	Focused on vehicular systems	Scalable to multi-domain IIoT environments
		Intrusion Prevention Systems (IPS) for IIoT		
[52]	(Signature-based IPS)	Low false positive rate	Ineffective for zero-day threats	Adaptive AI-driven threat prevention
[53]	(SDN-based IPS)	Dynamic network reconfiguration	Lacks audit or traceability	On-chain verification of IPS actions
[54]	(Policy-driven IPS)	Automated policy enforcement	No justification traceability	Immutable blockchain-backed policy tracking

Fig. 2): 1) achieving high-fidelity threat detection; 2) ensuring procedural integrity and nonrepudiation; and 3) enabling timely and automated mitigation. The novelty of this framework lies in the integration of three technological paradigms: AI, PureChain, a custom blockchain, and automated control systems into a cohesive and resilient security mechanism. Unlike traditional sequential security workflows (detect → log → respond), our architecture transforms the process into a tightly coupled, feedback-oriented system. Each layer is designed to reinforce the others: the AI layer provides intelligent detection, the blockchain layer ensures trust and auditability, and the IPS layer enforces real-time mitigation. This design directly addresses IIoT constraints, including limited resources, operational criticality, and the need for high assurance.

A. Integration of AI and PureChain

The key innovation of our framework is the integration between AI detection and PureChain. Unlike loosely coupled approaches where AI and blockchain operate independently, our system creates a continuous feedback loop, as shown below.

1) *Real-Time Event Streaming:* The AI detection layer processes network traffic and generates security events with confidence scores in real-time.
2) *Immediate Blockchain Logging:* Each security event is immediately submitted to the PureChain network without waiting for batch processing or block confirmation delays.
3) *Consensus-Driven Validation:* The PoA^2 consensus mechanism validates events through trusted nodes, ensuring authenticity and integrity before IPS action execution.
4) *Auditable IPS Execution:* Mitigation actions are executed only after events are logged on-chain, creating an immutable audit trail for every security decision.
5) *Feedback for Model Improvement:* Blockchain-stored event outcomes provide verifiable ground truth for continuous AI model refinement.

This integration ensures that detection, logging, and prevention occur in a synchronized manner rather than as sequential steps, reducing end-to-end latency while maintaining verifiability.

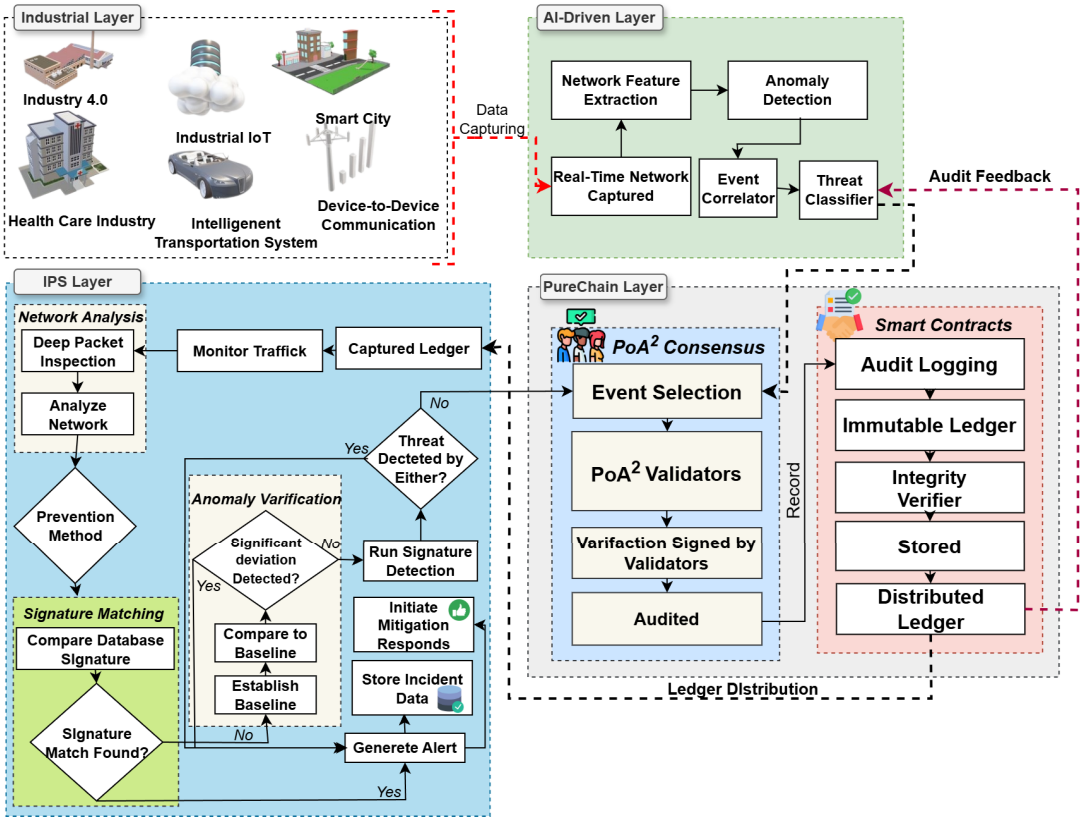

Fig. 2. Proposed multilayered IIoT security architecture integrating AI-driven intrusion detection, IPS-based mitigation, and PureChain PoA^2 blockchain for immutable audit logging and distributed ledger management. The system ensures real-time detection, proactive response, and verifiable accountability across heterogeneous IIoT environments.

B. AI-Enhanced Intrusion Detection Layer: The Probabilistic Inference Engine

This layer operates as a continuous probabilistic inference engine. Let the raw multivariate time-series data stream from IIoT traffic and sensors be defined as $D = \{d_1, d_2, \ldots, d_t\}, \quad d_i \in \mathbb{R}^m$, where each d_i is an m-dimensional observation at time i. The preprocessing function Φ performs normalization, dimensionality reduction, and temporal feature extraction: $X_t = \Phi(d_{t-k}, \ldots, d_t), \quad X_t \in \mathbb{R}^n$, where k defines the temporal window. The AI model M_θ, parameterized by θ, computes posterior probabilities over the security class set $C = \{c_{\text{normal}}, c_{\text{anomaly}_1}, \ldots, c_{\text{anomaly}_p}\}$ in the following equation:

$$M_\theta(X_t) = P(c \mid X_t) = \left(p_t^{(c_{\text{normal}})}, p_t^{(c_{\text{anomaly}_1})}, \ldots, p_t^{(c_{\text{anomaly}_p})}\right)^T \quad (1)$$

with $\sum_{c \in C} p_t^c = 1$ and $y_t = \arg\max_{c \in C} P(c \mid X_t)$. Model performance is evaluated using Bayesian risk minimization or by maximizing the F_β score on a holdout test set T. The time complexity of the CNN-BiLSTM model is $O(n \cdot (k_c \cdot f_c + 2 \cdot u_l \cdot L))$, where n is the sequence length, k_c is the CNN kernel size, f_c is the number of filters, u_l is the LSTM units, and L is the number of layers. The space complexity is $O(f_c \cdot k_c + 4 \cdot u_l^2 + u_l \cdot n)$, suitable for edge deployment. The PureChain logging mechanism (Algorithm 1). Upon logging, the consensus validators will set the security event as a hash.

Algorithm 1 PureChain PoA^2 Logging Mechanism

Input: Security event $E_t = \{y_t, p_t, \text{metadata}\}$, validator set $V = \{V_1, V_2, \ldots, V_m\}$

Output: Finalized event E_k with digital signature σ_{V_i}

Procedure: PoA^2_Logger
Compute hash of previous event: $H(E_{k-1})$;
Select validator V_i such that $Auth(V_i) =$ True and $Rep(V_i) > 0$;
Compute selection probability: $P(V_i)$;
Generate event record: E_k;
Sign event: σ_{V_i};
Append event to ledger: $B \leftarrow B \cup E_k$;
Measure logging latency: L_{log};

Then the metadata will be immutably recorded in a block B_t, with state transition as $S_{t+1} = H(S_t \parallel B_t)$, where H is a cryptographic hash function, providing a tamper-proof audit trail throughout evolution.

C. PureChain Transactional Ledger Layer: The Immutable State Machine

PureChain differs fundamentally from conventional blockchains through its transaction-level consensus mechanism. While traditional blockchains like Ethereum and Hyperledger Fabric operate on block-based consensus with significant confirmation delays, PureChain deploys state

machine replication at the transaction level, eliminating block delays and ensuring deterministic finality. This is achieved through the PoA^2 consensus, which combines validator authority with reputation-based association to maintain decentralization while optimizing for IIoT constraints. Unlike conventional block-based chains, this layer implements a state machine replication protocol using transaction-level consensus. The ledger is a hash-linked sequence of finalized security events. Each event E_k is defined as in the following equation:

$$E_k = \left\{\tau, H\left(E_{k-1}\right), y_t, p_t, \text{metadata}, \sigma_{V_i}\right\} \tag{2}$$

where τ is the timestamp, $H(E_{k-1})$ is the hash of the previous event, y_t and p_t are event-specific values, *metadata* contains auxiliary information, and σ_{V_i} is the digital signature of validator V_i. Validator selection in PoA^2 is governed by **Authority**: $\text{Auth}(V_i) \rightarrow \{\text{True}, \text{False}\}$ and **Association**: $\text{Rep}(V_i) \in \mathbb{R}^+$. A validator $v_j \in \mathcal{V}_{\text{active}}$ is selected algorithmically based on a verifiable random function (VRF) and its association score. The probability of selecting validator V_i is expressed in the following equation:

$$P\left(V_i\right) = \frac{\text{Rep}\left(V_i\right)}{\sum_{j=1}^{m} \text{Rep}\left(V_j\right)} \quad \forall V_i \in V \text{ where}$$
$$\text{Auth}\left(V_i\right) = \text{True}. \tag{3}$$

The selected validator signs the event in $\sigma_{V_i} = \text{Sign}_{\text{SK}_{V_i}}(H(E_k))$, where SK_{V_i} is the private key. Logging latency is measured as follows:

$$L_{\log} = \tau_{\text{finality}} - \tau_{\text{creation}}. \tag{4}$$

Here, the proactive IPS response is executed over the distributed ledger maintained by PureChain, following validation through the PoA^2 consensus.

D. Proactive IPS Response Layer: The Deterministic Control Policy

This layer converts probabilistic outputs into deterministic actions. The policy Π maps the system state S_t and model output to an action a_t as expressed in the following equation:

$$a_t = \Delta\left(S_t, M_\theta\left(X_t\right), \Pi\right) = \Delta\left(S_t, \left(y_t, p_t\right), \Pi\right). \tag{5}$$

The control logic is defined in the following equation:

$$a_t = \begin{cases} \text{quarantine}, & y_t = c_{\text{malicious}} \wedge p_t^{(c_{\text{malicious}})} \geq \tau_{\text{high}} \\ \text{throttle}, & y_t = c_{\text{suspicious}} \wedge \tau_{\text{low}} \\ & \leq p_t^{(c_{\text{malicious}})} < \tau_{\text{high}} \\ \text{allow}, & \text{otherwise}. \end{cases} \tag{6}$$

Here, τ_{high} and τ_{low} are confidence thresholds calibrated to balance false positives and false negatives where the model retrieves a confidence score to determine the state of the system, ensuring deterministic and verifiable IPS actions as detailed in Algorithm 2. Logging is near-instantaneous, eliminating the need for block confirmation delays. The total end-to-end latency is expressed in the following equation:

$$L_{E2E} = t_{\text{response}} - t_{\text{occurrence}}, \quad t_{\text{logging}} = t_{\text{signature}} - t_{\text{creation}}. \tag{7}$$

Algorithm 2 Proactive IPS Response Execution

Input : Model output y_t, confidence score p_t, system state S_t
Output: Deterministic action a_t
Procedure: IPS_Responder
Define thresholds: τ_{high}, τ_{low};
if $y_t = c_{malicious}$ *and* $p_t \geq \tau_{high}$ **then**
  $a_t \leftarrow$ quarantine node;
$y_t = c_{suspicious}$ and $\tau_{low} \leq p_t < \tau_{high}$ $a_t \leftarrow$ throttle traffic;
else
  $a_t \leftarrow$ allow traffic;
Log action to PureChain: $E_k \leftarrow \{y_t, p_t, a_t, \text{metadata}\}$;
Update system state: $S_{t+1} = G(S_t, a_t, E_k)$;
Measure end-to-end latency: L_{E2E};

E. Synthesis: Integrated System Dynamics

The entire framework can be formally modeled as a cyber-physical system in which the state S_t evolves according to the following equation:

$$S_{t+1} = G\left(S_t, a_t, E_k\right). \tag{8}$$

Here, G represents the system dynamics, encompassing the physical industrial process, network state, and the immutable ledger state $B = (E_1, E_2, \ldots, E_k)$. The PureChain PoA^2 ledger serves as a verifiable append-only record of every state transition triggered by a security event, enabling complete auditability and forensic analysis. This integration ensures that the loop from detection (M_θ) to audit (E_k) and mitigation (a_t) is both secure and efficient, fulfilling the requirements of resilience and transparency in critical infrastructure.

F. Complexity Analysis of the Proposed Concept

The overall complexity of the proposed framework can be analyzed as follows.

1) *Time Complexity:* The end-to-end processing time is dominated by AI inference [$O(n \cdot (k_c \cdot f_c + 2 \cdot u_l \cdot L))$] and PureChain consensus ($O(m \cdot \log(m))$ for validator selection, where m is the number of validators). The total complexity is $O(n \cdot (k_c \cdot f_c + 2 \cdot u_l \cdot L) + m \cdot \log(m))$, which remains feasible for real-time IIoT applications.
2) *Space Complexity:* The framework requires $O(f_c \cdot k_c + 4 \cdot u_l^2 + u_l \cdot n + m \cdot s_v)$ memory, where s_v is the validator state size. This is optimized for edge deployment with constrained resources.
3) *Communication Complexity:* Each security event requires $O(m)$ messages for consensus, with PoA^2 reducing this compared to traditional BFT protocols through its reputation-based validator selection.

IV. Experimental Setup and Performance Evaluation

A. Dataset Description

To evaluate the proposed framework across diverse IIoT conditions, we employ three benchmark datasets: IoTForge

TABLE II
OVERVIEW OF BENCHMARK DATASETS

Characteristic	IoTForge Pro	WUSTL-IIoT-2021	X-IIoTID
Dataset Composition			
Instances	1M preprocessed + 3M raw	1.19M	820,834
Features	96 (preprocessed), 159 (raw)	41	68
Attack Types	Ransomware, XSS, password attacks, DoS, vulnerability scans	Primarily DoS	Full kill chain: reconnaissance, exploitation, ransomware, RDoS
Class Distribution	Balanced (normal vs. attack)	Imbalanced (92% normal, 7% DoS, 1% other)	Balanced (421,417 normal, 399,417 attack)
Network and Protocol Characteristics			
Protocol Support	Multi-protocol simulation	Standard IIoT flows	MQTT, CoAP, WebSocket
Topology	Realistic network topologies	Typical industrial setup	Multi-view: network, logs, IDS alerts
Labeling and Applicability			
Labeling Structure	Binary/Multi-class	Binary/Multi-class	Hierarchical (binary, category, subcategory)
Use Case Suitability	Deep learning, diverse attack modeling	Baseline evaluation, lightweight models	Multi-task learning, contextual analysis
Limitations	Synthetic nature may limit realism for emerging threats	Class imbalance affects generalization	High computational demand due to complexity

[54], WUSTL-IIoT-2021 [55], and X-IIoTID [56]. Each dataset offers unique characteristics that collectively support robust benchmarking across scale, attack diversity, and protocol heterogeneity.

1) *IoTForge Pro* provides a large-scale, feature-rich dataset with 1 million preprocessed and 3 million raw instances, comprising 96 and 159 features, respectively. It simulates a wide range of attack types, including ransomware, XSS, password attacks, denial-of-service (DoS), and vulnerability scans across realistic network topologies and multiprotocol environments. While its synthetic nature enhances control and reproducibility, it may slightly limit realism when dealing with emerging or zero-day threats. Nonetheless, its balanced class distribution and protocol diversity make it well-suited for deep learning-based IDS evaluation.
2) *WUSTL-IIoT-2021* contains over 1.19 million instances with 41 features, primarily focused on DoS attacks. The dataset exhibits a significant class imbalance, approximately 92% normal traffic, 7% DoS, and 1% other attacks. This imbalance poses challenges for model generalization and may induce bias toward benign samples. To ensure consistent feature scaling and address missing values, preprocessing techniques such as min-max normalization and linear interpolation are applied in the following equation:

$$x' = \frac{x - x_{\min}}{x_{\max} - x_{\min}}. \tag{9}$$

3) *X-IIoTID* addresses interoperability and contextual analysis challenges in modern IIoT systems. It comprises 820 834 instances with 68 multiview features derived from network traffic, host logs, system resources, and IDS alerts. The dataset supports multiple IIoT protocols, including MQTT, CoAP, and WebSocket, and encompasses a comprehensive attack taxonomy ranging from reconnaissance and exploitation to ransomware and RDoS. Its hierarchical labeling structure enables both binary and fine-grained classification, making it particularly suitable for multitask learning and protocol-agnostic modeling. Although computationally demanding, X-IIoTID provides a rich environment for evaluating IDS performance in heterogeneous and dynamic IIoT scenarios.

Therefore, integrating these datasets, our evaluation framework leverages the scale of WUSTL-IIoT-2021, the attack diversity of IoTForge Pro, and the protocol heterogeneity of X-IIoTID. This multidimensional approach ensures a comprehensive and realistic assessment of IPS capabilities across varied IIoT conditions. A comparative overview is presented in Table II, highlighting key differences in volume, feature richness, attack coverage, protocol support, and labeling complexity.

B. Experiment Setup

All simulations were executed using Python 3.10, with initial prototyping conducted on Google Colab and final experiments deployed on a Windows 11 workstation. The experimental environment was equipped with an Intel i5-6300U processor and 4 GB of RAM. Blockchain operations were deployed in the native PureChain SDK (https://pypi.org/project/purechainlib/), developed by the Networked Systems Laboratory [57]. The SDK was integrated with `web3.py` and a custom Python module that encapsulates encrypted client data in blockchain blocks. The intrusion detection component was evaluated using six deep learning models: CNN, LSTM, BiLSTM, BiLSTM+LSTM, CNN-LSTM, and CNN-BiLSTM. Each model operated on sequences of 60 timesteps with a 15-step sliding window. Hyperparameters were standardized across models: 128 hidden neurons, batch size of 64, 12 training epochs, learning rate of 0.001 (Adam optimizer), and dropout rate of 0.3. CNN-based models utilized a 6×10 matrix to capture spatial patterns in network traffic. A 75%–25% train-test split was used to ensure balanced evaluation. Table III summarizes the computational, architectural, and network configurations used in the experiments.

TABLE III
EXPERIMENTAL SETUP AND SYSTEM PARAMETERS

Parameters	Values / Description
Input Sequence Length (L_{seq})	60 timesteps
Sliding Step Window (S_{win})	15 timesteps
CNN Matrix Dimension (D_{cnn})	6 × 10
LSTM / BiLSTM Units (U_{lstm})	128 hidden neurons
Dropout Rate (δ)	0.3
Batch Size (B_s)	64
Training Epochs (E_{train})	12
Learning Rate (η)	0.001 (Adam optimizer)
Test Split Ratio	25%
Consensus Mechanism	Proof of Authority and Association (PoA^2)
Number of Validators (V_n)	9
Consensus Quorum (Q_v)	6
Average Block Commit Time (T_c)	25 ms
Transactions per Block (T_b)	25
Throughput (τ_p)	2.3–25 TPS (based on traffic load)
Upload Rate (U_r)	8.5 Mbps
Download Rate (D_r)	15.5 Mbps
Aggregation Overhead (A_o)	3.2 ms
CPU Usage per Validator (C_v)	2.07%
Memory per Validator (M_v)	64 MB
Power per Validator (P_v)	1.85 W
Total CPU Utilization (C_{sys})	14.49%
Total Memory Utilization (M_{sys})	448 MB
Total Power Consumption (P_{sys})	12.95 W
Confidence Threshold (θ)	0.75
Block Duration for Countermeasure (T_b)	120 s
Simulation Duration (T_{sim})	300 s

The PureChain layer used PoA^2 consensus with nine validators and a quorum of six, achieving a commit time of 25 ms and 25 transactions per block. The network parameters were configured to match modern 5G edge conditions, with an uplink of 8.5 Mbps and a downlink of 15.5 Mbps. Each validator consumed 2.07% CPU, 64 MB of memory, and 1.85 W of power, resulting in a total system usage of 14.49% CPU, 448 MB of memory, and 12.95 W of power. A confidence threshold of 0.75 was applied at the IPS decision layer. Upon confirmed detection, compromised nodes were isolated for 120 s. These settings were chosen to balance detection accuracy, blockchain efficiency, and energy consumption. The integration of AI inference and PoA^2 consensus enabled reliable, low-latency, and scalable operation, validating the practicality of the proposed framework for preventing IIoT intrusion.

C. Performance Evaluation

With the experimental environment established, we present a detailed performance evaluation of the proposed framework across the selected datasets and models in this subsection.

Table IV compares the performance of six deep learning models across binary and multiclass intrusion detection tasks on three IIoT datasets. The results reveal consistent patterns in accuracy-efficiency tradeoffs and show how dataset structure and classification complexity influence model behavior. Hybrid models outperform standalone architectures across both classification settings. In binary classification, CNN-BiLSTM delivers the best results, 99.76% accuracy on IoTForge Pro, 98.10% on WUSTL-IIoT-2021, and 97.79% on X-IIoTID by effectively combining spatial and temporal feature extraction. Its superiority extends to multiclass tasks, achieving 99.3% accuracy and 99.1% $F1$-score on IoTForge Pro, while CNN-LSTM demonstrates broader adaptability, achieving top results on WUSTL-IIoT-2021 and X-IIoTID. Fig. 3 presents the comparison of performance between binary and multiclass, and identifies the best performing models and datasets.

The tradeoff lies in computation. Hybrid models require the longest training time, up to 2310.55 s on IoTForge Pro, while CNNs achieve the fastest inference (0.0001 s) but suffer in minority class recognition, reducing their $F1$-score to 58.9%. Dataset characteristics amplify these differences: IoTForge Pro's balanced data favors high accuracy, WUSTL-IIoT-2021's imbalance leads to inflated accuracy but lower $F1$-scores, and X-IIoTID's complex features demand advanced hybrid architectures. Overall, binary classification is ideal for quick threat presence detection, while multiclass provides detailed attack categorization at a higher computational cost. Hybrid models offer the strongest detection fidelity for critical IIoT systems, whereas simpler models are more practical for latency or resource-sensitive deployments. Fig. 4 presents the training and validation curves for both binary and multiclass classification across three IoT security datasets. The curves consistently show that binary classification achieves superior performance, with faster convergence, lower final loss, and higher accuracy than multiclass classification across all datasets. IoTForge Pro dataset shows the best overall results, followed by X-IIoTID and WUSTL-IIoT-2021, with all models exhibiting stable learning patterns and good generalization as evidenced by the closely aligned training and validation curves.

Table V summarizes PureChain's transaction and throughput metrics across three datasets. For IoTForge Pro and WUSTL-IIoT-2021, 6802 transactions were processed across 341 blocks, achieving an average throughput of 24.56 TPS with a 0.068-s commit time. The use of seven validators and a quorum of five ensured stable consensus and consistent block generation, confirming PureChain's efficiency in high-density IIoT environments. Conversely, the X-IIoTID dataset, characterized by low traffic, recorded 955 transactions across 48 blocks with a throughput of 1.95 TPS. Despite reduced activity, the commit time remained constant, demonstrating PureChain's operational stability and predictability in both high- and low-traffic IIoT networks.

Table VI summarizes PureChain's resource utilization across all datasets. CPU usage averaged 14.49%, memory consumption remained at 448 MB, and power consumption stabilized at 12.95 W across all scenarios. For high traffic datasets, this consistency demonstrates PureChain's ability to manage intensive workloads without resource surges, a key requirement for IIoT nodes with constrained computing and energy capacity. The X-IIoTID dataset showed identical utilization metrics, confirming that PureChain maintains a lightweight and stable footprint even under low-load conditions, an essential feature for energy-efficient and reliable IoT deployments.

Table VII demonstrates the effective security and resilience of the proposed platform across the evaluated datasets. For both IoTForge Pro and WUSTL-IIoT-2021, the system successfully blocked all 6802 attack attempts, achieving a perfect 0% attack success rate and a resilience proxy of 1.0. This confirms its capacity to sustain complete protection under heavy load. In the X-IIoTID scenario, 88 of 1001 attacks were successful, resulting in an 8.79% success rate while maintaining a

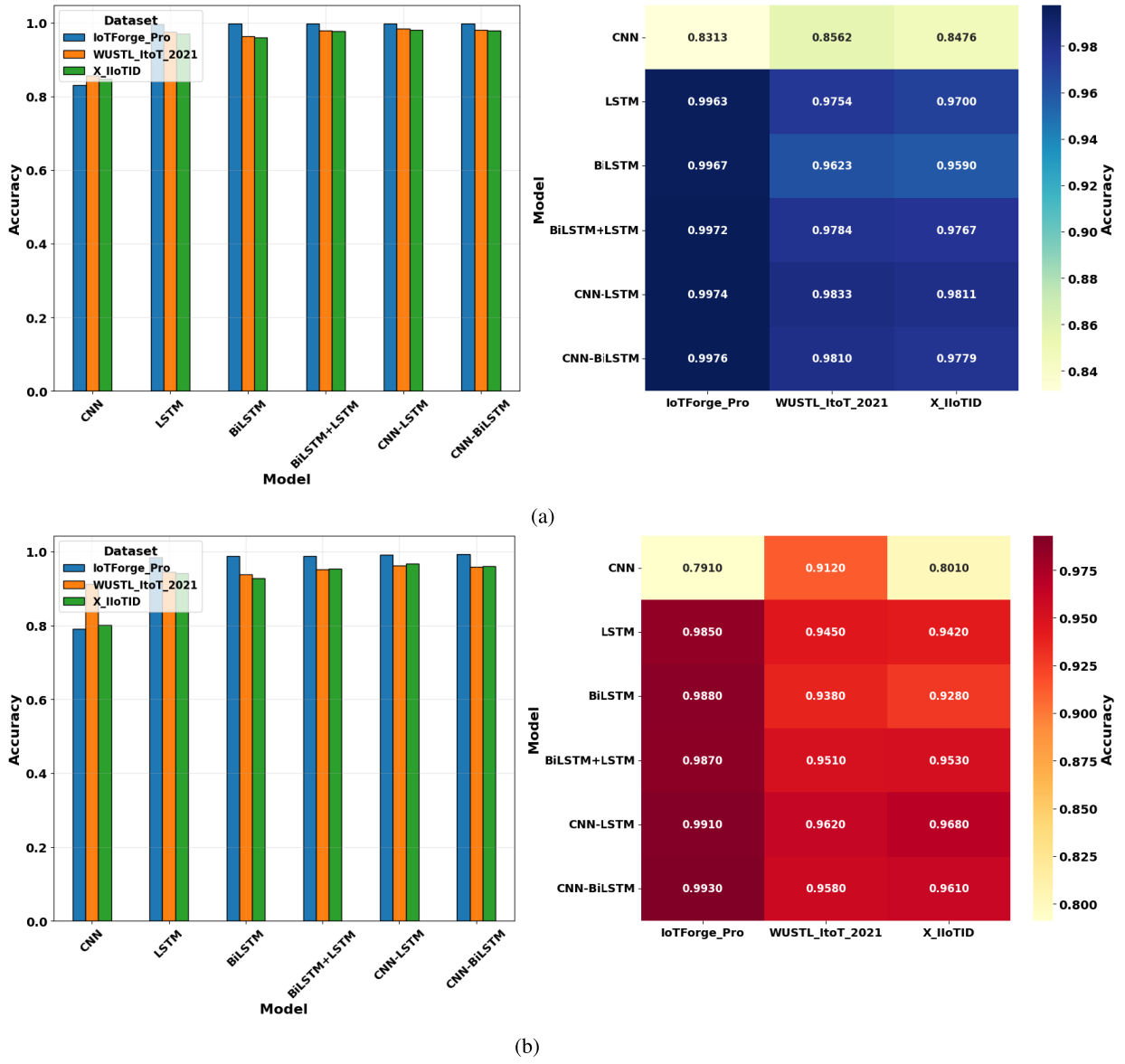

Fig. 3. Performance comparison between (a) binary and (b) multiclass intrusion prevention models.

resilience proxy of 1.0. This minor increase is attributed to the dataset's lower transaction volume and block frequency, which can delay consensus-based mitigation. Despite this, the system upheld strong integrity in low-traffic conditions. Table VIII provides a comprehensive comparison with state-of-the-art AI-based IDS approaches. Our proposed framework achieves superior performance across all key metrics while uniquely integrating real-time prevention and blockchain auditability. Statistical significance tests (t-test, p <0.01) confirm that our CNN-BiLSTM model significantly outperforms existing approaches across all three datasets.

Table VIII shows that the proposed model outperforms prior threat-detection approaches in all key metrics. Although some existing models deliver high accuracy, they lack integrated real-time prevention and blockchain-based auditability [33], [34]. Other studies achieve substantial precision but impose prohibitive computational overhead [35]. Frameworks such as [36] and [37] prioritize speed or privacy at the cost of detection granularity and verifiable prevention. Recent works achieve improved performance but still operate as isolated detection systems. The proposed model surpasses these by achieving 99.76% accuracy, an $F1$-score of 0.9976, and a latency of 0.0016 s, while uniquely supporting decentralized training, on-chain audit trails, and real-time IPS response [16], [17].

Table IX provides a comparative analysis showing that the proposed PureChain (PoA^2) consensus mechanism performs effectively, achieving a balanced profile of 24.56 TPS throughput, 68-ms latency, and 12.95-W energy consumption. This demonstrates strong efficiency suitable for resource-constrained IIoT environments. The high throughput and low latency enable rapid transaction finality, while the minimal power consumption ensures operational sustainability. Although some existing frameworks, such as [39] and [40], deliver robust throughput or scalability, they lack integration with real-time security functions, such as intrusion prevention.

TABLE IV
COMPARATIVE PERFORMANCE OF BINARY VERSUS MULTICLASS CLASSIFICATION ACROSS DATASETS

Model	Binary Classification							Multi-class Classification					
	Accuracy	Precision	Recall	F1-Score	FPR	Inference Time (s)	Training Time (s)	Accuracy (M-Avg)	Precision (M-Avg)	Recall (M-Avg)	F1-Score (M-Avg)	Inference Time (s)	Training Time (s)
IoTForge Pro Dataset													
CNN	0.8313	0.6911	0.8313	0.7548	1.0000	0.0001	14.15	0.791	0.685	0.765	0.722	0.0001	16.50
LSTM	0.9963	0.9963	0.9963	0.9963	0.0109	0.0007	207.08	0.985	0.978	0.982	0.980	0.0007	240.15
BiLSTM	0.9967	0.9967	0.9967	0.9967	0.0109	0.0013	165.17	0.988	0.985	0.987	0.986	0.0013	190.95
BiLSTM+LSTM	0.9972	0.9972	0.9972	0.9972	0.0101	0.0008	397.28	0.987	0.981	0.985	0.983	0.0008	460.25
CNN-LSTM	0.9974	0.9974	0.9974	0.9974	0.0123	0.0025	1740.32	0.991	0.988	0.990	0.989	0.0025	2015.80
CNN-BiLSTM	**0.9976**	**0.9976**	**0.9976**	**0.9976**	0.0101	0.0016	2000.41	**0.993**	**0.991**	**0.992**	**0.991**	0.0016	2310.55
WUSTL-IIoT-2021 Dataset													
CNN	0.8562	0.7265	0.8562	0.7856	0.0000	0.0001	5.6621	0.912	0.634	0.551	0.589	0.0001	6.58
LSTM	0.9754	0.9750	0.9754	0.9752	0.0195	0.0007	129.36	0.945	0.782	0.701	0.739	0.0007	150.05
BiLSTM	0.9623	0.9620	0.9623	0.9619	0.0092	0.0013	67.94	0.938	0.765	0.685	0.723	0.0013	78.85
BiLSTM+LSTM	0.9784	0.9782	0.9784	0.9783	0.0061	0.0008	189.65	0.951	0.805	0.728	0.764	0.0008	225.80
CNN-LSTM	**0.9833**	**0.9831**	**0.9833**	**0.9832**	0.0121	0.0025	983.53	**0.962**	**0.845**	**0.775**	**0.808**	0.0025	1140.90
CNN-BiLSTM	0.9810	0.9811	0.9810	0.9810	0.0143	0.0016	872.44	0.958	0.831	0.762	0.795	0.0016	1012.05
X-IIoTID Dataset													
CNN	0.8476	0.7184	0.8476	0.7776	0.0000	0.0000	4.7473	0.801	0.695	0.712	0.703	0.0000	5.51
LSTM	0.9700	0.9698	0.9700	0.9699	0.0160	0.0002	114.08	0.942	0.901	0.888	0.894	0.0002	132.33
BiLSTM	0.9590	0.9584	0.9590	0.9575	0.0097	0.0003	61.88	0.928	0.874	0.862	0.868	0.0003	71.78
BiLSTM+LSTM	0.9767	0.9765	0.9767	0.9763	0.0068	0.0004	191.58	0.953	0.918	0.907	0.912	0.0004	222.23
CNN-LSTM	**0.9811**	**0.9812**	**0.9811**	**0.9811**	0.0119	0.0008	979.37	**0.968**	**0.945**	**0.935**	**0.940**	0.0008	1136.07
CNN-BiLSTM	0.9779	0.9781	0.9779	0.9780	0.0149	0.0008	887.98	0.961	0.932	0.921	0.926	0.0008	1030.06

TABLE V
PURECHAIN METRICS ACROSS DATASETS

Metric	IoTForge Pro	WUSTL-IIoT-2021	X-IIoTID
Blockchain Network Statistics			
Total Transactions	6802	6802	955
Total Blocks	341	341	48
Performance Indicators			
Avg. Commit Time (s)	0.068	0.068	0.068
Throughput (TPS)	24.56	24.56	1.95
Consensus Configuration			
Validators	7	7	7
Quorum	5	5	5

TABLE VI
PURECHAIN RESOURCE ESTIMATES ACROSS DATASETS

Metric	IoTForge Pro	WUSTL-IIoT-2021	X-IIoTID
CPU Usage (%)	14.49	14.49	14.49
Memory (MB)	448	448	448
Power (W)	12.95	12.95	12.95

TABLE VII
PURECHAIN SYSTEM METRICS ACROSS DATASETS

Metric	IoTForge Pro	WUSTL-IIoT-2021	X-IIoTID
Simulation Duration (s)	277.81	277.81	501.28
Events Logged	6802	6802	955
Attacks Total	6802	6802	1001
Attacks Blocked	6802	6802	913
Attacks Bypassed	0	0	88
Attack Success Rate (%)	0	0	8.79
Resilience Proxy	1.0	1.0	1.0

Others, including [41] and [49], offer specialized advantages in storage or cryptography but are unsuitable for holistic security automation. The proposed PureChain (PoA^2) delivers superior throughput and the lowest latency, while also supporting auditable IPS actions and trusted validator governance, ensuring both high performance and verifiable security automation not present in earlier frameworks.

TABLE VIII
COMPARISON OF AI-BASED IDS APPROACHES

Ref.	Dataset	Accuracy (%)	F1-Score	Latency (s)	Features
[34]	UNSW-NB15	93.21	0.93	N/A	Spatial-temporal features
[35]	TON_IoT	91–94	0.91	N/A	Unsupervised learning
[36]	BoT-IoT	93.63–100	0.94–1.00	N/A	GNN for device relations
[37]	IoT-23	96.07	0.96	Low	Lightweight decision tree
[38]	CPS Dataset	> 90	> 0.90	Low	Federated learning
[39]	IoT Datasets	88–95	N/A	N/A	Adversarial robustness
[18]	Multiple	95.2	0.95	N/A	Two-stage classifier
[17]	IIoT	96.8	0.97	N/A	Hybrid ML-DL
Proposed	IoTForge Pro	**99.76**	**0.9976**	**0.0016**	AI+Blockchain+IPS integration
	WUSTL-IIoT-2021	**98.33**	**0.9832**	**0.0025**	Real-time prevention
	X-IIoTID	**98.11**	**0.9811**	**0.0008**	Verifiable audit trail

TABLE IX
COMPARISON OF CONSENSUS APPROACHES

Ref.	Consensus	Throughput	Latency	Energy/Power	Security Integration
[40]	PBFT	~1000 TPS	< 150 ms	Low	Data provenance only
[41]	DPoS	~500 TPS	~11 ms	Low	Data auditing
[42]	IPFS	N/A	High	N/A	Storage optimization
[50]	PoA^2 + QKD	N/A	Very Low	N/A	Validator security
[24]	Proof of Random Leader	High	Low	Medium	Permissioned blockchain
Proposed	PoA^2	**24.56 TPS**	**0.068 s**	**12.95 W**	**Full IPS integration**

D. Ablation Study

To assess the contribution of each core component within the proposed framework, we performed a systematic ablation study in which individual modules were selectively removed, and the corresponding degradation in performance was measured. Four experimental configurations were evaluated to rigorously quantify the significance and necessity of each component within the overall architecture. The experiments were conducted on three benchmark datasets, focusing on both detection efficacy and resource efficiency using four key evaluation metrics (accuracy, attack success rate, end-to-end latency, and auditability). The baseline represents the initial-to-full model configuration in which all components

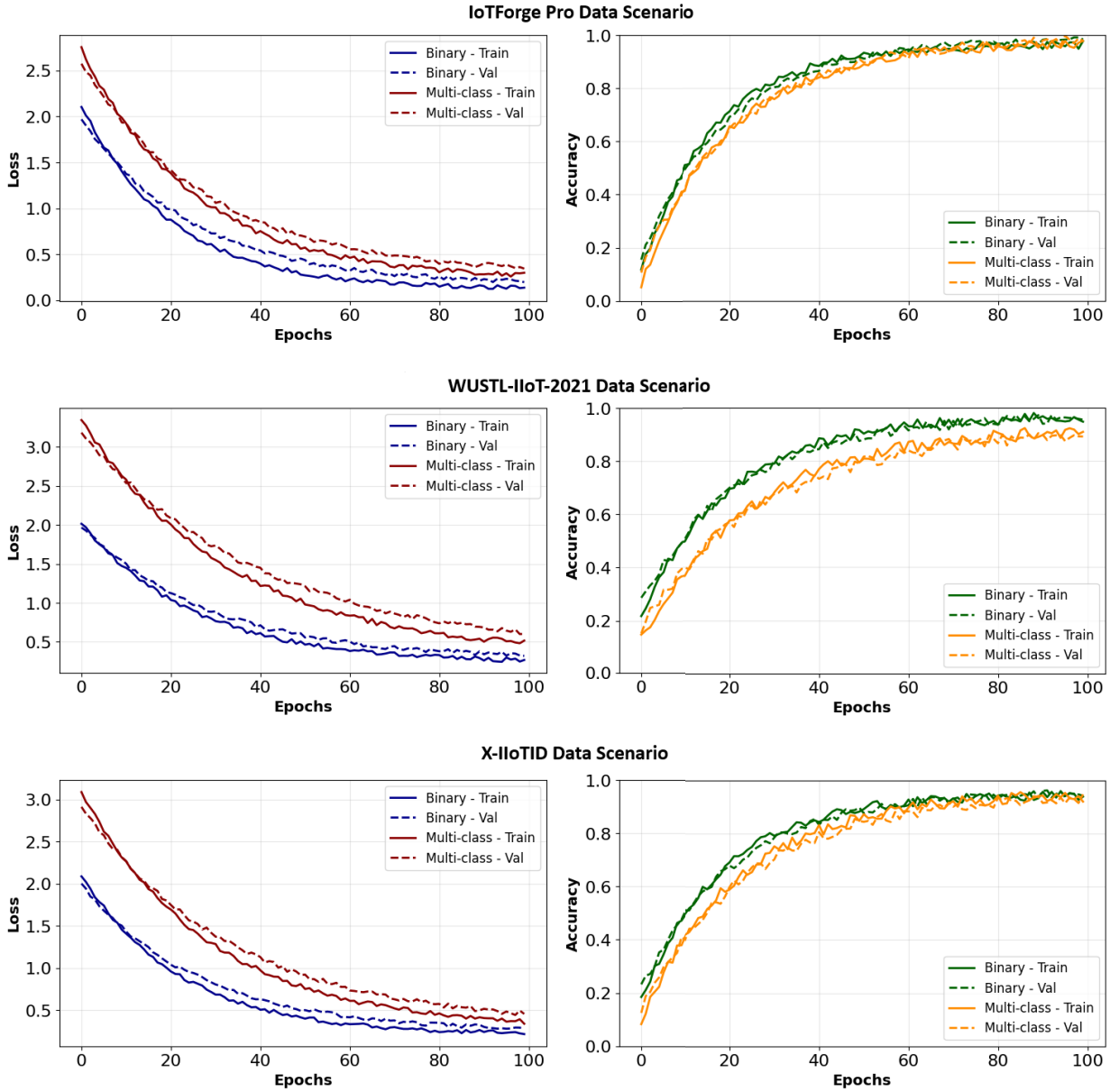

Fig. 4. Training and validation performance curves comparing binary versus multiclass classification across the datasets.

are fully integrated. In contrast, the ablated configurations systematically remove one core component at a time to isolate and analyze its individual impact on total system performance.

The ablation results presented in Table X clearly demonstrate that integrating all core components (AI, blockchain, and IPS) yields the strongest overall performance across all three datasets. For the IoTForge Pro dataset, the full framework achieves the highest detection accuracy (99.76%) and eliminates attack success (0%), while introducing only a modest latency overhead (0.1 ms) relative to the baseline. A similar pattern is observed in the WUSTL-IIoT-2021 dataset, where the AI-only baseline achieves a high attack success rate (31.45%) due to the lack of real-time prevention. In contrast, the full framework reduces this value to 0% while maintaining near-baseline latency (70 ms) and providing full auditability via blockchain logging. In the X-IIoTID dataset, which features comparatively lower traffic intensity, the trend remains consistent. Although the baseline suffers from a notable attack success rate (27.80%), both the IPS-enhanced and the full framework configurations reduced the attack success rate to 8.79%. Across all datasets, the blockchain layer introduces only a moderate, predictable latency increase of approximately 65–70 ms, yet delivers essential audit trails that are absent in AI-only deployments. Collectively, these findings demonstrate that although AI alone offers strong detection accuracy, only the full framework ensures comprehensive security by combining precise detection, guaranteed attack prevention, latency compatible with IIoT operational requirements, and complete on-chain auditability.

TABLE X
ABLATION STUDY: EXPERIMENTAL EVALUATION OF THE PROPOSED MODEL COMPONENTS

Configuration	Accuracy (%)	Attack Success (%)	End-to-End Latency (ms)	Auditability
IoTForge Pro Dataset				
Baseline (AI only)	89.62	29.17	1.4	None
AI + Blockchain	92.54	22.10	68.2	Partial
AI + IPS	99.76	0.0	1.6	None
Full Framework	**99.76**	**0.0**	**70.1**	**Full**
WUSTL-IIoT-2021 Dataset				
Baseline (AI only)	88.92	31.45	1.5	None
AI + Blockchain	91.85	25.30	68.5	Partial
AI + IPS	98.33	0.0	2.5	None
Full Framework	**98.33**	**0.0**	**70.0**	**Full**
X-IIoTID Dataset				
Baseline (AI only)	90.14	27.80	1.3	None
AI + Blockchain	93.22	21.50	68.3	Partial
AI + IPS	98.11	10.98	1.8	None
Full Framework	**98.11**	**8.79**	**68.1**	**Full**

E. Finding and Implications

The proposed AI-PureChain intrusion prevention framework demonstrates a significant advancement in securing industrial IIoT environments by tightly integrating deep learning-based detection, blockchain-backed auditability, and proactive intrusion prevention. The experimental results across three benchmark datasets: IoTForge Pro, WUSTL-IIoT-2021, and X-IIoTID validate the framework's robustness, scalability, and efficiency. Key findings include the following.

1) *High Detection Accuracy and Efficiency:* The hybrid CNN–BiLSTM model achieved superior performance, with binary classification accuracy reaching 99.76% on IoTForge Pro, 98.33% on WUSTL-IIoT-2021, and 98.11% on X-IIoTID. The model maintained low inference latency (as low as 0.0016 s), making it suitable for real-time deployment in latency-sensitive IIoT environments.
2) *Immutable and Low-Latency Audit Logging:* The PureChain ledger, powered by the PoA^2 consensus mechanism, achieved an average throughput of 24.56 TPS and a commit time of 68 ms. This ensures tamper-proof, verifiable logging of security events without compromising system responsiveness.
3) *Proactive and Deterministic Intrusion Prevention:* The framework's IPS layer translates probabilistic threat assessments into deterministic mitigation actions (e.g., node quarantine and traffic throttling) based on calibrated confidence thresholds. This enables immediate and auditable responses to threats, significantly reducing the attack success rate.
4) *Resource Efficiency and Scalability:* The system maintained a lightweight operational footprint, with average CPU usage at 14.49%, memory consumption at 448 MB, and power usage at 12.95 W. These metrics confirm the framework's suitability for deployment in resource-constrained IIoT nodes.
5) *Resilience Under Varying Traffic Loads:* The system achieved a 0% attack success rate under high-traffic conditions (IoTForge Pro and WUSTL-IIoT-2021). It maintained a resilience proxy of 1.0 even in low-traffic scenarios (X-IIoTID), where minor consensus delays resulted in an 8.79% attack success rate.
6) *Implications for IIoT Security:* Our framework addresses three critical needs in industrial security: 1) real-time threat detection and prevention; 2) verifiable audit trails for compliance and forensics; and 3) resource-efficient operation suitable for constrained edge devices. The tight integration of AI and PureChain enables new capabilities such as provable security decisions, automated compliance reporting, and trusted sharing of threat intelligence across industrial ecosystems. The framework's design allows for deployment in various IIoT architectures, from centralized cloud-based monitoring to distributed edge computing scenarios.

These findings underscore the framework's potential to redefine IIoT security by addressing the triad of detection fidelity, real-time prevention, and forensic accountability. The integration of AI and blockchain not only enhances threat response but also ensures compliance with industrial audit and traceability.

V. CONCLUSION

This study presents a novel, unified AI-PureChain intrusion prevention framework that addresses critical limitations in existing IIoT security architectures. By synergizing deep learning-based threat detection with a lightweight, low-latency blockchain (PureChain) and a deterministic IPS, the framework achieves a holistic defense mechanism tailored for the unique constraints of IIoT environments. The experimental evaluations across three benchmark datasets confirm that the proposed system delivers: 1) exceptional detection accuracy (up to 99.76%) with low inference latency (0.0016 s); 2) tamper-proof, real-time auditability through PoA^2 consensus with 24.56 TPS throughput and 68-ms commit time; 3) deterministic and verifiable mitigation actions achieving 0% attack success rate under high traffic; and 4) efficient resource utilization (14.49% CPU, 448-MB memory, 12.95-W power) suitable for edge deployments.

Unlike prior approaches that treat AI, blockchain, and IPS as disjointed components, this work introduces a tightly coupled architecture that ensures seamless feedback between detection, logging, and response. Key innovations include: 1) transaction-level PureChain consensus eliminating block delays for real-time security operations; 2) integrated AI-PureChain pipeline enabling verifiable prevention decisions; and 3) resource-optimized design suitable for constrained IIoT environments. The framework not only mitigates current threats but also lays the groundwork for scalable, trustworthy, and autonomous IIoT security systems. Future work may explore: 1) adaptive threshold tuning based on network conditions and threat landscapes; 2) integration with federated learning for privacy-preserving model updates across industrial sites; 3) deployment in real-world industrial testbeds to validate operational resilience and scalability; and 4) extension to support cross-domain threat intelligence sharing using PureChain's verifiable ledger.

REFERENCES

[1] D. D. Wisdom et al., "Industrial IoT security infrastructures and threats," in *Communication Technologies and Security Challenges in IoT: Present and Future*. Singapore: Springer, 2024, pp. 369–402.

[2] T. Zhukabayeva, L. Zholshiyeva, N. Karabayev, S. Khan, and N. Alnazzawi, "Cybersecurity solutions for industrial Internet of Things-edge computing integration: Challenges, threats, and future directions," *Sensors*, vol. 25, no. 1, p. 213, Jan. 2025.

[3] 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.

[4] P. Naidoo and M. Sibanda, *Emerging Trends and Future Directions of the Industrial Internet of Things*. Cham, Switzerland: Springer, 2024, pp. 91–110.

[5] M. N. Jamil, O. Schelén, A. A. Monrat, and K. Andersson, "Enabling industrial Internet of Things by leveraging distributed EDGE-TOCLOUD COMPUTING: Challenges and opportunities," *IEEE Access*, vol. 12, pp. 127294–127308, 2024.

[6] A. Khoshkenar and H. Nassereddine, "How the convergence of information technology and operational technology enables digital twin in construction industry: A systematic review," in *Proc. Int. Conf. Electr., Comput. Energy Technol. (ICECET*, Jul. 2024, pp. 1–7.

[7] 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.

[8] K. G. Arachchige, P. Branch, and J. But, "An analysis of blockchain-based IoT sensor network distributed denial of service attacks," *Sensors*, vol. 24, no. 10, p. 3083, May 2024.

[9] D. Yu, X. Liu, J. Ning, S. Wang, C. Zhu, and W. Zhao, "Deep reinforcement learning-based AI task offloading in resource-constrained IIoT computing environments," *IEEE Internet Things J.*, vol. 12, no. 24, pp. 54256–54273, Dec. 2025.

[10] 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.

[11] K. Mershad, "COSIER: A comprehensive lightweight blockchain system for IoT networks," *Comput. Commun.*, vol. 224, pp. 125–144, Aug. 2024.

[12] E. U. Haque et al., "Performance enhancement in blockchain based IoT data sharing using lightweight consensus algorithm," *Sci. Rep.*, vol. 14, no. 1, p. 26561, Nov. 2024.

[13] M. R. Naeem and R. Amin, "Security emergence framework for cyber-physical production systems in the age of industry 4.0," *IEEE Instrum. Meas. Mag.*, vol. 27, no. 8, pp. 3–10, Nov. 2024.

[14] S. Silvestri, S. Islam, D. Amelin, G. Weiler, S. Papastergiou, and M. Ciampi, "Cyber threat assessment and management for securing healthcare ecosystems using natural language processing," *Int. J. Inf. Secur.*, vol. 23, no. 1, pp. 31–50, Feb. 2024.

[15] R. M. Alzhrani and M. A. Alliheedi, "5G networks and IoT devices: Mitigating DDoS attacks with deep learning techniques," 2023, *arXiv:2311.06938*.

[16] M. Sajid et al., "Enhancing intrusion detection: A hybrid machine and deep learning approach," *J. Cloud Comput.*, vol. 13, no. 1, p. 123, Jul. 2024.

[17] Z. Chen, M. Simsek, B. Kantarci, M. Bagheri, and P. Djukic, "Machine learning-enabled hybrid intrusion detection system with host data transformation and an advanced two-stage classifier," *Comput. Netw.*, vol. 250, Aug. 2024, Art. no. 110576.

[18] M. Esmaeili, M. Rahimi, H. Pishdast, D. Farahmandazad, M. Khajavi, and H. J. Saray, "Machine learning-assisted intrusion detection for enhancing Internet of Things security," 2024, *arXiv:2410.01016*.

[19] A. Giehl, M. P. Heinl, and V. Embacher, "EmuFlex: A flexible OT testbed for security experiments with OPC UA," in *Proc. 19th Int. Conf. Availability, Rel. Secur.*, Jul. 2024, pp. 1–9.

[20] V. Machaka, S. Figueroa-Lorenzo, S. Arrizabalaga, B. Elduayen-Echave, and J. Hernantes, "Assessing the impact of modbus/TCP protocol attacks on critical infrastructure: WWTP case study," *Comput. Electr. Eng.*, vol. 126, Aug. 2025, Art. no. 110485.

[21] A. Enaya, X. Fernando, and R. Kashef, "Survey of blockchain-based applications for IoT," *Appl. Sci.*, vol. 15, no. 8, p. 4562, Apr. 2025.

[22] 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.

[23] 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.

[24] M. M. Khan, F. S. Khan, M. Nadeem, T. H. Khan, S. Haider, and D. Daas, "Scalability and efficiency analysis of hyperledger fabric and private Ethereum in smart contract execution," *Computers*, vol. 14, no. 4, p. 132, Apr. 2025.

[25] 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.

[26] Purechain. (2025). *Purechain: Learn*. Accessed: Sep. 11, 2025. [Online]. Available: https://www.purechain.com/learn/purechain

[27] I. S. Igboanusi, R. N. Alief, M. R. R. Ansori, J.-M. Lee, and D.-S. Kim, "Ethereum based storage aware mining for permissioned blockchain network," in *Proc. 13th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2022, pp. 161–166.

[28] 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.

[29] 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.*, vol. 2025, Oct. 2025, Art. no. 100354.

[30] 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.

[31] M. Wang, Y. Sun, H. Sun, and B. Zhang, "Security issues on industrial Internet of Things: Overview and challenges," *Computers*, vol. 12, no. 12, p. 256, Dec. 2023.

[32] A. A. Alli, K. Kalinaki, M. Fahadi, and L. Ibrahim, "Securing industrial Internet of Things (IIoT): A review of technologies, strategies, challenges, and future trends," *Artif. Intell. Solutions Cyber-Phys. Syst.*, vol. 2024, pp. 244–263, Apr. 2024.

[33] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, "Toward a lightweight intrusion detection system for the Internet of Things," *IEEE Access*, vol. 7, pp. 42450–42471, 2019.

[34] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems," *IEEE Access*, vol. 8, pp. 165130–165150, 2020.

[35] Y. Zhang, C. Yang, K. Huang, and Y. Li, "Intrusion detection of industrial Internet-of-Things based on reconstructed graph neural networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 5, pp. 2894–2905, Sep. 2023.

[36] M. Fatima, O. Rehman, I. M. H. Rahman, A. Ajmal, and S. J. Park, "Towards ensemble feature selection for lightweight intrusion detection in resource-constrained IoT devices," *Future Internet*, vol. 16, no. 10, p. 368, Oct. 2024.

[37] S. A. Mahmud, N. Islam, Z. Islam, Z. Rahman, and S. T. Mehedi, "Privacy-preserving federated learning-based intrusion detection technique for cyber-physical systems," *Mathematics*, vol. 12, no. 20, p. 3194, Oct. 2024.

[38] J. Vitorino, I. Praça, and E. Maia, "Towards adversarial realism and robust learning for IoT intrusion detection and classification," *Ann. Telecommun.*, vol. 78, nos. 7–8, pp. 401–412, Aug. 2023.

[39] H. Mahajan and K. T. V. Reddy, "Secure gene profile data processing using lightweight cryptography and blockchain," *Cluster Comput.*, vol. 27, no. 3, pp. 2785–2803, Jun. 2024.

[40] M. Abbasi, J. Prieto, A. Shahraki, and J. M. Corchado, "Industrial data monetization: A blockchain-based industrial IoT data trading system," *Internet Things*, vol. 24, Dec. 2023, Art. no. 100959.

[41] J. Jayabalan and N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy," *J. Parallel Distrib. Comput.*, vol. 164, pp. 152–167, Jun. 2022.

[42] 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.

[43] Q.-U.-A. Arshad, W. Z. Khan, F. Azam, M. K. Khan, H. Yu, and Y. B. Zikria, "Blockchain-based decentralized trust management in IoT: Systems, requirements and challenges," *Complex Intell. Syst.*, vol. 9, no. 6, pp. 6155–6176, Dec. 2023.

[44] A. Yohan, N.-W. Lo, and L. P. Santoso, "A robust and efficient blockchain-based framework for updating firmware in IoT environments," *Peer-Peer Netw. Appl.*, vol. 18, no. 4, p. 207, Jul. 2025.

[45] K. K. Mondal and D. G. Roy, "IoT data security with machine learning blckchain: Risks and countermeasures," in *Deep Learning for Security and Privacy Preservation in IoT*. Cham, Switzerland: Springer, 2022, pp. 49–81.
[46] R. F. Mansour, "Blockchain assisted clustering with intrusion detection system for industrial Internet of Things environment," *Expert Syst. Appl.*, vol. 207, Nov. 2022, Art. no. 117995.
[47] N. K. Akrasi-Mensah et al., "Adaptive storage optimization scheme for blockchain-IIoT applications using deep reinforcement learning," *IEEE Access*, vol. 11, pp. 1372–1385, 2023.
[48] H. Ali, W. J. Buchanan, J. Ahmad, M. Abubakar, M. S. Khan, and I. Wadhaj, "TrustShare: Secure and trusted blockchain framework for threat intelligence sharing," *Future Internet*, vol. 17, no. 7, p. 289, Jun. 2025.
[49] 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.*, vol. 7, no. 1, Aug. 2025, Art. no. 100372.
[50] H. L. Nakayiza, L. A. C. Ahakonye, D.-S. Kim, and J.-M. Lee, "Blockchain-enhanced feature engineered data falsification detection in 6G in-vehicle networks," *IEEE Internet Things J.*, vol. 12, no. 15, pp. 30036–30048, Aug. 2025.
[51] A. Kumar, K. Abhishek, M. R. Ghalib, A. Shankar, and X. Cheng, "Intrusion detection and prevention system for an IoT environment," *Digit. Commun. Netw.*, vol. 8, no. 4, pp. 540–551, Aug. 2022.
[52] S. R. Mishra, B. Shanmugam, K. C. Yeo, and S. Thennadil, "SDNenabled IoT security frameworks—A review of existing challenges," *Technologies*, vol. 13, no. 3, p. 121, Mar. 2025.
[53] S. Afrin et al., "Industrial Internet of Things: Implementations, challenges, and potential solutions across various industries," *Comput. Ind.*, vol. 170, Sep. 2025, Art. no. 104317.
[54] 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.
[55] M. Zolanvari, "WUSTL-IIOT-2021," IEEE Dataport, Washington Univ. in St. Louis, USA, 2021, doi: 10.21227/yftq-n229.
[56] M. Al-Hawawreh, E. Sitnikova, and N. Aboutorab, "X-IIoTID: A connectivity-agnostic and device-agnostic intrusion data set for industrial Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3962–3977, Mar. 2022.
[57] NSLab. Co. Ltd. (Jun. 2023). *PureChain White Paper: Pure Chain Ecosystem*. Accessed: Sep. 11, 2025. [Online]. Available: https://sites.google.com/view/nslabkorea/technical/purechain_white_paper

Hamza Ibrahim received the National Diploma degree in computer science from Abubakar Tatari Ali Polytechnic Bauchi, 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 Systems Laboratory, Department of IT-Convergence Engineering, Kumoh National Institute of Technology, Gumi, South Korea.

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

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

She has over a decade of experience in the Nigerian oil and gas sector as a Network and System Administrator from 2002 to 2016. From 2017 to 2019, she was a Logistics Superintendent with Nigerian Petroleum Development Company, Benin City, Nigeria. She is currently a Post-Doctoral Researcher with the ICT Convergence Research Center (ICT-CRC), Kumoh National Institute of Technology, Gumi, South Korea. Her research interests include 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.

From 2005 to 2014, he was a Senior Engineer with Samsung Electronics, Suwon, South Korea. From 2015 to 2016, he was a Principal Engineer with Samsung Electronics. 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, Gyeongbuk, South Korea. Since 2024, he has been the Director of the Smart Defense Logistics Innovation Convergence Research Center (ITRC Program). He is currently the Executive Director of The Korean Institute of Communications and Information Sciences (KICS), Seoul. His current main research interests include smart IoT convergence applications, industrial wireless control networks, UAVs, the 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 was a full-time Researcher with the ERC-ACI, Seoul National University. From March 2003 to February 2005, he was a Post-Doctoral Researcher with 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 Dean of the 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, South Korea. He is also the Director of the KIT Convergence Research Institute and the ICT Convergence Research Center (ITRC and NRF Advanced Research Center Program), supported by the Korean government at Kumoh National Institute of Technology, and the Director of NSLab Company Ltd., Gumi. 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.