PureChain-Based Intrusion Detection and Prevention System for Secure Industrial Internet of Things

Hamza Ibrahim [1], Love Allen Chijioke Ahakonye [2], Jae Min Lee [1], Dong-Seong Kim [1] *
[1] IT-Convergence Engineering, *Kumoh National Institute of Technology*, Gumi, South Korea
* NSLab Co. Ltd., Gumi, South Korea, *Kumoh National Institute of Technology*, Gumi, South Korea
[2] ICT Convergence Research Center, *Kumoh National Institute of Technology*, Gumi, South Korea
(hamza, loveahakonye, ljmpaul, dskim) @kumoh.ac.kr

***Abstract*—The Industrial Internet of Things (IIoT) intrusions require beyond-detection systems due to their damaging effects. There is a need for a combined intrusion detection and prevention (IDPS) mechanism to ensure complete protection of these critical systems. This study proposes a PureChain-based framework for IIoT to maintain an immutable ledger and a proactive, real-time threat detection and mitigation. The experiments demonstrate low latency, high throughput, minimal resource utilization, and effective attack prevention, showcasing the scalability and suitability of the PureChain for secure IIoT environments.**

***Index Terms*—Blockchain, Industrial IoT, Intrusion Prevention System, PureChain, PoA^2, Security.**

I. Introduction

Securing Industrial Internet of Things (IIoT) devices remains challenging due to their resource constraints and growing exposure to complex cyber threats [1]. Traditional centralized models fall short, highlighting the need for lightweight, decentralized, and resilient protection frameworks [2]. Blockchain offers a promising foundation by ensuring immutable integrity, transparency, and distributed trust, making it well-suited for intrusion detection systems (IDS) [3]. However, detection alone is not enough; coupling IDS with intrusion prevention systems (IPS) enables both the identification and real-time mitigation of threats, thereby strengthening IIoT security [4].

Research shows a move from reactive IDS to proactive IPS, highlighting the need for adaptive, automated defenses [5]. Hybrid approaches combining deep learning and blockchain [4], as well as low-latency DL-based IPS for 5G/6G networks [6], set the stage. Building on this, this study integrates PureChain with IPS, offering a secure, efficient, and blockchain-verifiable solution for IIoT. Using Proof of Authority and Association (PoA^2) consensus applied at the transaction level [7], PureChain eliminates block delays, ensures deterministic finality, and delegates heavy validation to trusted nodes, addressing the blockchain "quad-lemma" of decentralization, security, scalability, and cost [8]. This design supports scalable, energy-efficient IIoT IDPS deployments.

II. Methodology

Figure 1 shows the PureChain with PoA^2 consensus mechanism to validate IIoT security logs and create immutable records. Alerts flow to a proactive IPS, which evaluates threats and executes smart contract-driven mitigation actions, such as device isolation or IP blocking, while logging all actions on the PureChain. This design ensures transparent accountability, fast response, and robust protection for IIoT edge devices. For evaluation, we used IoTForge Pro [9], which simulates synthetic and real-world attacks. Security events E_k, represented as $E_k = \big(\tau, H(E_{k-1}), y_t, p_t, \text{metadata}, \sigma_{V_i}\big)$ encode timestamp τ, previous event hash output, metadata, and validator signature which are selected based on reputation of prior event via PoA^2 protocol validator as $V = \{V_1, V_2, \ldots, V_m\}$ for each event E_k. A validator V_i is selected through a deterministic function f that incorporates validator reputation $R(V_i)$ and the previous event hash $V_i \sim f\big(R(V_1), R(V_2), \ldots, R(V_m), H(E_{k-1})\big)$. The designated validator verifies the event and signs it $\sigma_{V_i} = \text{Sign}_{SK_{V_i}}\big(H(E_k)\big)$. Logging latency remains in milliseconds, enabling near real-time validation. The decision function Δ maps the state of the system and the output to actions a_t from the permissible set $A = \{\text{allow}, \text{quarantine}, \text{shutdown}, \text{throttle}\}$: $a_t = \Delta\big(S_t, (y_t, p_t), \Pi\big)$, where the governing policy Π is implemented as threshold-based rules in Equation 1.

$$a_t = \begin{cases} \text{quarantine}, & \text{if } (y_t = c_{malicious}) \wedge \big(p_t^{(c_{malicious})} \geq \tau_{high}\big) \\ \text{throttle}, & \text{if } (y_t = c_{suspicious}) \wedge \big(\tau_{low} \leq p_t^{(c_{malicious})} < \tau_{high}\big) \\ \text{allow}, & \text{otherwise} \end{cases} \tag{1}$$

Using calibrated thresholds τ_{high} and τ_{low} to balance false positives and negatives. End-to-end latency $L_{E2E} = t_{response} - t_{occurrence}$ covers detection, logging, and mitigation, ensuring secure and timely responses in IIoT deployments.

III. Evaluation Performance

Table I shows PureChain achieving 24.56 TPS with 0.068 s latency using 7 validators (quorum of 5). Validators required just 2.07% CPU, 64 MB memory, and 1.85 W power, keeping total system use at 14.5% CPU, 448 MB, and 13 W. Across 278 seconds and 6,802 events, PureChain blocked 100% of attacks with a resilience score of 1.0. Table II highlights that, unlike prior works focused mainly on accuracy or modest scalability, PureChain combines complete attack blocking, blockchain-backed performance (24.56 TPS, 0.068 s

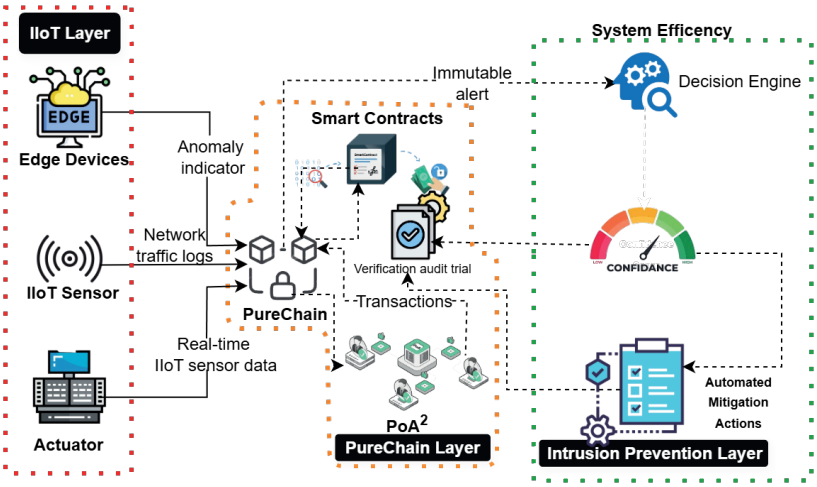

Fig. 1. PureChain Pipeline Process

latency), and low resource costs, offering real-time prevention, scalability, and resilience for IIoT.

TABLE I
SYSTEM METRICS

Category	Metric	Result
PureChain Metrics	Throughput (TPS)	24.56
	Latency (Avg Commit Time)	∼0.068 s per block
	Validators and Quorum	7 validators, quorum = 5
	Scalability & Fault Resilience	Supported
Resource Estimates	Per-validator Load (CPU)	2.07%
	Per-validator Memory	64 MB
	Per-validator Power	1.85 W
	Total System Load (CPU)	∼14.5%
	Total System Memory	448 MB
	Total System Power	∼13 W
System Metrics	Simulation Duration	∼278 s
	Logged Events	6802
	Security Outcome	100% attacks blocked, 0% success rate
	Resilience Proxy	1.0

TABLE II
COMPARATIVE PERFORMANCE OF IDS/IPS APPROACHES

Ref.	Accuracy (%)	Scalability	Efficiency	Mitigation / Latency	Real-Time
[6]	99.9	Not reported	Not reported	Optimized processing speed	Partial
[4]	96.8%	92.5%	91.7%	90.8%	Yes
Proposed (PureChain)	**100 (attacks blocked)**	**24.56 TPS; 7 validators (quorum=5)**	**CPU 2.07%; Mem 64 MB; Power 1.85 W**	**∼0.068s; Resilience Proxy = 1.0**	**Yes**

IV. CONCLUSION

We presented a PureChain–based intrusion detection and prevention framework for securing IIoT systems. The system utilizes PoA^2 consensus mechanism for tamper-proof logging with low latency and high throughput, while the IDPS layer enables real-time detection, automated mitigation, and auditable responses. The results show minimal resource overhead, 100% attack blocking, and a resilience score of 1.0. Future work will scale the framework to larger IIoT networks, integrate adaptive approaches, and validate it on real-world testbeds.

ACKNOWLEDGMENT

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korea government (MSIT) (IITP-2025-RS-2020-II201612, 33%) and by Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003, 33%) and by the MSIT, Korea, under the ITRC support program (IITP-2025-RS-2024-00438430, 34%).

REFERENCES

[1] Z. Alwaisi, T. Kumar, E. Harjula, and S. Soderi, "Securing Constrained IoT Systems: A Lightweight Machine Learning Approach for Anomaly Detection and Prevention," *Internet of Things*, vol. 28, p. 101398, 2024.

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

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

[4] M. Srinivasan and N. C. Senthilkumar, "Intrusion Detection and Prevention System (IDPS) Model for IIoT Environments Using Hybridized Framework," *IEEE Access*, vol. 13, pp. 26 608–26 621, 2025.

[5] M. Markevych and M. Dawson, "A Review of Enhancing Intrusion Detection Systems for Cybersecurity using Artificial Intelligence (AI)," in *International conference knowledge-based organization*, vol. 29, no. 3, 2023, pp. 30–37.

[6] K. Mavale, A. Ingle, C. M. Reddy, and P. D. Honawadajkar, "An Intelligent Hybrid Intrusion Detection and Prevention System for Threat Mitigation in High Bandwidth 5G/6G Network," in *Proceedings of the International Conference on Emerging Trends in Communication and Computing*. IEEE, 2025, pp. 1–6.

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

[8] D.-S. Kim, I. S. Igboanusi, L. A. C. Ahakonye, and G. O. Anyanwu, "Proof-of-Authority-and-Association Consensus Algorithm for IoT Blockchain Networks," in *The 43rd IEEE International Conference on Consumer Electronics (ICCE 2025)*, 2025, pp. 1–6.

[9] 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 of Things Journal*, vol. 12, no. 7, pp. 8453–8460, 2025.