A Decentralized Approach to Tamper-Proof SCADA Intrusion Detection and Prevention System

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

***Abstract*—The convergence of SCADA and IoT expands attack surfaces while straining real-time defenses. Traditional intrusion detection systems suffer from centralized control, tamper risks, and weak trust models. We propose a PureChain-based SCADA–IoT approach that employs a custom blockchain for immutable logging, decentralized trust, and secure prevention. The framework combines signature and anomaly-based detection with ML models, achieving rapid mitigation and auditable response. Evaluations reveal a performance of accuracy–efficiency trade-offs, with PureChain ensuring low commit times (0.067s), stable throughput, and minimal resource utilization (2.07% CPU, 64 MB/validator). Results confirm its scalability and robustness for securing critical SCADA–IoT infrastructures.**

***Index Terms*—Intrusion detection, Prevention, PoA^2, PureChain, SCADA.**

I. Introduction

Supervisory Control and Data Acquisition (SCADA), increasingly integrated with IoT devices, is vital to critical infrastructure but faces heightened cyber risks due to expanded attack surfaces and real-time operational demands [1]. Conventional intrusion detection systems, while central to defense, are insufficient to prevent attacks, data tampering, and logging manipulation [2]. These limitations hinder timely and trustworthy detection and response, especially in distributed SCADA–IoT environments, where adversaries can exploit weak nodes or disrupt centralized monitoring [3].

Blockchain provides a decentralized, immutable, and transparent foundation to enhance the integrity of data, distribute intrusion alerts, and prevent log manipulation, thereby improving both detection reliability and prevention effectiveness [4]. While recent studies have explored blockchain-based anomaly detection, alert sharing, and hybrid ML intrusion detection and prevention systems (IDPS), performance trade-offs, particularly in terms of latency, remain a challenge in SCADA networks [4], [5]. This work extends these efforts by examining how blockchain integration can strengthen SCADA–IoT IDPS, offering resilient, trustworthy, and scalable protection against evolving cyber threats.

II. System Methodology

This study proposes a SCADA–IoT IDPS, as shown in Figure 1, that integrates PureChain [6] for storing hashed data and flow statistics, thereby providing tamper-proof evidence to ensure integrity and accountability throughout packet capture,

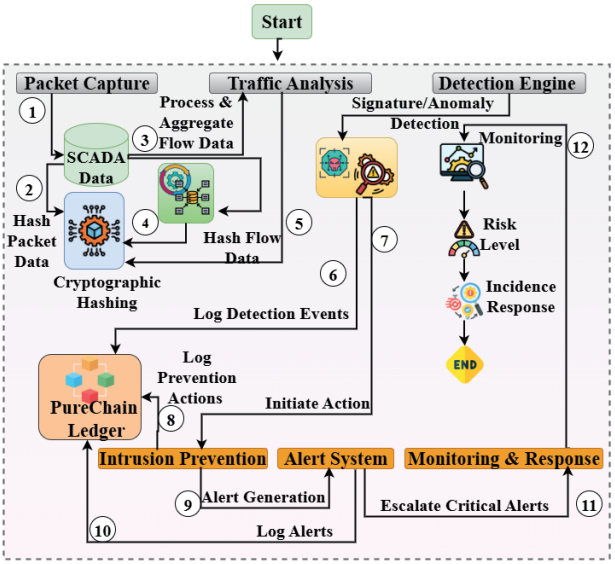

Fig. 1. Design details of the proposed PureChain-based IDPS architecture illustrating the interaction of the involved entities.

traffic analysis, detection, alerting, and prevention. The system follows a flow described by the Equation 1.

$$\forall s \in \{C, A, D, P, L\}: \quad \begin{cases} C \xrightarrow{\mathcal{H}} A \xrightarrow{\mathcal{H}} D \xrightarrow{d=0} C, \\ C \xrightarrow{\mathcal{H}} A \xrightarrow{\mathcal{H}} D \xrightarrow{d=1} (P \parallel L) \to C. \end{cases} \quad \wedge \quad s \dashrightarrow \overset{\log}{\underset{\text{async}}{}} \tag{1}$$

where C represents data capture, A is analysis, D is detection, P is prevention, L is system alert, B is PureChain, $d \in \{0, 1\}$ represents the detection decision (0 = benign, 1 = malicious), $\parallel$ denotes parallel execution, and $\dashrightarrow \overset{\log}{\underset{\text{async}}{}}$ represents asynchronous PureChain logging. Signature detection matches flow features F against known attack patterns as shown in Equation 2.

$$\mathcal{D}_{sig}(F) = \begin{cases} 1 & \text{if } \exists \sigma \in \quad : \sigma \subseteq F, \\ 0 & \text{otherwise}, \end{cases} \tag{2}$$

while anomaly detection evaluates deviations from a baseline model, as in Equation 3.

$$\mathcal{D}_{anom}(F) = \begin{cases} 1 & \text{if } \alpha(F) \geq \theta, \\ 0 & \text{otherwise.} \end{cases} \quad (3)$$

The detection engine uses both signature-based and machine learning-based anomaly detection to cover known and novel threats. When a threat is detected ($\delta = 1$), an alert AL is triggered, and a prevention action A (e.g., IP blocking or device isolation) is executed. Both actions are securely logged on the PureChain, ensuring complete threat coverage, fast response, and tamper-proof auditability.

III. Experimental Results and Discussion

The proposed framework was evaluated using two IoT intrusion detection datasets, comprising seven PureChain validators and detection models (Random Forest, LSTM, and BiLSTM). Table I shows that Random Forest achieves optimal performance with the fastest training times of 150.9s for ForgedIoT, and 184.7s for WUSTL. LSTM and BiLSTM demonstrated high accuracy, albeit at the expense of longer training time. Random Forest offers the best performance-efficiency balance, while LSTM and BiLSTM are better suited for complex sequential data at a higher computational cost.

TABLE I
Model Evaluation

Data Scenario	Model	Acc	Prec	Rec	Fscore	FPR	Train time (s)
WUSTL	Random Forest	1	1	1	1	0	184.7
	LSTM	0.9993	0.9993	0.9993	0.9993	0	334.5
	BiLSTM	0.9993	0.9993	0.9993	0.9993	0.0002	158.8
ForgedIoT	Random Forest	0.9998	0.9998	0.9998	0.9998	0.0009	150.9
	LSTM	0.9963	0.9963	0.9963	0.9963	0.0109	207.0
	BiLSTM	0.9967	0.9967	0.9967	0.9967	0.0109	165.1

Table II illustrates the PureChain evaluation, illustrating notable differences in transaction volume and throughput. It shows significance in transacting varying degrees of data volumes (6,802 ForgedIoT Pro) at a rate of 24.5591 transactions per second, and (686 WUSTL-IIoT-2021) at a rate of 2.2874 transactions per second, highlighting the system's scalability. Both setups maintain similar commit times (0.067 seconds), relying on 7 validators with a 5-member quorum, ensuring consistent performance and resilience in transaction validation.

TABLE II
PureChain Evaluation

Data Scenario	Total transactions	Total blocks	Average commit (s)	Throughput (tps)	No of validators	Quorum
WUSTL	686	35	0.0676	2.2874	7	5
ForgedIoT	6802	341	0.0679	24.5591	7	5

Table III presents resource utilization estimates for PureChain, exhibiting identical resource profiles. It requires approximately 2.07% CPU, 64 MB memory, and 1.85 W power per validator node. At the system level, this scales to 14.49% CPU, 448 MB total memory, and 12.95 W total power consumption, reflecting the aggregate requirements for the validation process of seven (7) utilized validators. It demonstrates that PureChain maintains consistent resource efficiency across distinct IoT benchmark datasets, highlighting its scalability and predictability in deployment scenarios.

TABLE III
PureChain Resource Estimate

Data Scenario	CPU Usage/ Validator (%)	Memory/Usage/ Validator (MB)	Power Usage/ Validator (W)
WUSTL	2.07	64	1.85
ForgedIoT	2.07	64	1.85

IV. Conclusion

This study introduced a PureChain-based SCADA–IoT IDPS that leverages blockchain immutability and hybrid detection to overcome the limitations of conventional systems in distributed, latency-sensitive environments. Results show Random Forest delivers the best balance of accuracy and efficiency, while LSTM models remain suitable for complex sequential threats at a higher cost. PureChain further ensures scalable, low-overhead, and energy-efficient operation, validating its suitability for large-scale SCADA–IoT deployments. Overall, the framework provides a resilient and auditable cybersecurity solution for protecting critical infrastructures against evolving adversarial threats.

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (IITP-2025-RS-2020-II201612, 40%), the Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2018R1A6A1A03024003, 30%), by the Institute of Information & Coummunications Technology Planning & Evaluation (IITP)-ITRC(Information Technology Research Center) grant funded by the Korea government(Ministry of Science and ICT)(IITP-2025-RS-2024-00438430 30%)

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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," *Journal of Communications and Networks*, vol. 26, no. 1, pp. 65–79, 2024.

[6] 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.