Synergistic Blockchain and Zero Trust Framework for Securing Industrial IoT Against Cyber Threats

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 of Technology*, Gumi, South Korea
(hmzibrahim30@gmail.com, (loveahakonye, ljmpaul, dskim)@kumoh.ac.kr

***Abstract*—Traditional perimeter-based security models are insufficient for securing Industrial Internet of Things (IIoT) networks, which are inherently dynamic, distributed, and continually exposed to evolving cyber threats. This study proposes a secure and scalable framework that integrates Zero Trust (ZT) architecture with PureChain, a custom blockchain platform designed to enhance IIoT cybersecurity. At the core of PureChain is a novel Proof of Authority and Association (PoA^2) consensus mechanism, enabling low-latency and energy-efficient operations. The framework enforces security policies through smart contracts and evaluates device behavior using real-time trust scores. An LSTM-based anomaly detection engine provides proactive threat identification, enabling adaptive and intelligent security responses. The system is evaluated using two benchmark IIoT datasets: WUSTL-IIoT-2021 and IoTForge Pro, and demonstrates superior performance compared to existing blockchain platforms and consensus mechanisms across key metrics, including throughput, latency, scalability, energy consumption, and detection accuracy. The results validate that the proposed PureChain-ZT framework delivers a practical, robust, and adaptive solution for real-time IIoT security, particularly in resource-constrained and high-risk industrial environments.**

***Index Terms*—Anomaly Detection, Blockchain, IIoT, PoA^2, PureChain, Zero Trust**

I. Introduction

As cyber threats continue to evolve, traditional perimeter-based security models are no longer sufficient. These models assume that internal networks are inherently trustworthy, an assumption that is increasingly invalid in today's dynamic infrastructures, which involve cloud computing, the Internet of Things (IoT), and the Industrial Internet of Things (IIoT) [1]. The increasing sophistication of attacks and the dynamic nature of modern infrastructures have exposed the limitations of these conventional approaches [2]. Therefore, there is a rising demand for advanced security frameworks that not only protect against external threats but also address internal vulnerabilities and enforce security across every layer of the network [3].

Zero Trust (ZT) has emerged as a solution to these shortcomings by fundamentally challenging the traditional concept of trust in network security. ZT operates on the principle of "never trust, always verify," ensuring that all users, devices, and services are continuously authenticated and authorized, regardless of their location within the network. (see Figure 1) [4]. This approach has been recognized as essential to

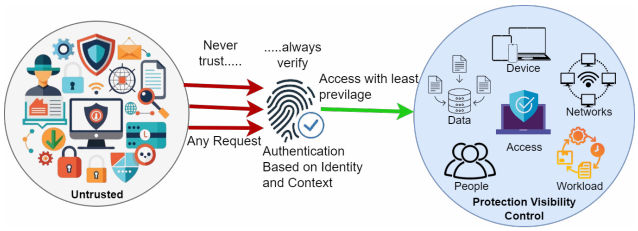


Fig. 1: Zero Trust

mitigate the risks associated with data breaches, insider threats, and unauthorized access [5]. ZT is particularly effective in environments where the network is no longer limited to the perimeter but extends to a distributed cloud-based infrastructure [6].

Blockchain complements ZT by providing decentralized and immutable data management solutions that can significantly improve network security [2], [7]. The distributed ledger system on blockchain ensures the integrity of data and transactions, which makes it an ideal solution to securely log access attempts, validate user identities, and maintain an immutable audit trail [8]. Therefore, by incorporating blockchain into a ZT framework, organizations can further reinforce trust verification and ensure that security events are recorded in a tamper-proof manner [2]. Furthermore, the inherent properties of blockchain, such as transparency, accountability, and decentralization, address many vulnerabilities in traditional systems, such as a single point of failure and the potential for unauthorized data manipulation [9].

This study presents a secure and scalable IIoT framework by integrating ZT with PureChain, a custom blockchain that leverages an enhanced proof-of-authority with association (PoA^2) consensus mechanism [10]. In this system, only pre-validated nodes create and validate blocks, utilizing a multi-factor scoring system that combines historical performance, system metrics, and real-time behavioral analysis. This approach reduces energy use compared to proof-of-work and improves efficiency validation. The key contributions of this paper are as follows:

1) We present a framework that integrates ZT with PureChain, a custom blockchain, to create a secure and decentralized network for dynamic IIoT, ensuring con-

tinuous authentication and tamper-proof data logging.
2) A comprehensive evaluation and analysis of PureChain with Ethereum, Hyperledger, and PoA^2 with other consensus mechanisms, offering insights into the performance trade-offs in terms of throughput, latency, energy consumption, and scalability.
3) We provide an extensive performance analysis of the concept, demonstrating its applicability in real-world IIoT environments with high scalability, efficiency, and real-time threat mitigation.

Following Section I is Section II, which reviews the current literature on blockchain and ZT integration in IIoT. Section III details the architecture of the proposed framework, which combines blockchain and ZT, designed to address the challenges of cyber attacks in securing IIoT systems. Section IV presents experimental results and performance analysis. Finally, Section V concludes the paper and outlines future work directions.

II. Background and Related Work

Industrial IoT enhances operational efficiency through real-time data, automation, and analytics; however, its growing connectivity introduces significant cybersecurity challenges [11]. In response, researchers have explored ZT, which enforces continuous verification and context-aware access control. Although several studies have attempted to integrate blockchain with ZT, they exhibit key limitations. For instance, Awan et al. [12] proposed a blockchain-based access control system, but lacked support for real-time threat detection and scalability. Li et al. [13] introduced BasIoT for identity management in 5G-enabled IIoT but did not address adaptive threat response or resource limitations.

Similarly, Nie et al. [14] designed a complex ZT model for 6G-IoT, which is unsuitable for resource-constrained IIoT devices. Bobde et al. [15] integrated encryption with PoA consensus, but their approach fell short in scalability and real-time responsiveness. Nazir et al. [16] proposed a blockchain-ML framework for collaborative detection, although it remains largely theoretical. Verma et al. [17] emphasized the potential of blockchain within ZT but did not validate it within practical IIoT environments. Collectively, these studies are limited by their conceptual focus, lack of real-time capabilities, or cloud-centric assumptions.

This highlights the need for a unified architecture with low latency, scalability, and energy efficiency for IIoT security. While machine learning has been explored for threat detection [18], no solution fully integrates Zero Trust and blockchain. We introduce PureChain, a blockchain framework that combines Zero Trust with a novel PoA^2 consensus. It improves throughput, reduces latency and energy consumption, and supports AI-driven anomaly detection and real-time security enforcement, offering a comprehensive solution for dynamic IIoT environments.

III. Proposed Methodology

The proposed framework integrates blockchain with ZT principles to enhance cybersecurity in IIoT systems. As shown in Figure 2, dynamic trust scores securely stored on the blockchain govern access control decisions. The blockchain logs access events and triggers smart contract-based actions, such as revoking access, updating trust levels, and alerting administrators. An anomaly detection engine generates risk signals that feed both the access control and blockchain layers, ensuring synchronized threat response. The PoA^2 consensus protocol enables fast, reliable validation with low latency and high data integrity across nodes.

A. BZTF-Based IIoT Cyber Threat Detection Workflow

In the proposed blockchain-based ZT model, access control enforces the principle of least privilege by dynamically evaluating trust scores. Each device D_i, when requesting access at time t, is assigned a real-time trust score as $T_i(t) = f(H_i, C_i, A_i)$, where H_i: historical behavior stored immutably on the blockchain, C_i: current contextual data (IP, location, time), A_i: anomaly risk score from the anomaly detection engine. This engine actively monitors system behavior and raises an alert if it detects suspicious activity. The risk signal is defined as $R_i(t) = \mathbb{1}[\text{anomaly detected for } D_i \text{ at time } t]$ where the indicator function returns 1 if an anomaly is found and 0 otherwise. However, access control decisions are enforced using smart contracts. If a device trust score falls below a threshold τ, the smart contract immediately revokes access, records the event on the blockchain, and notifies the system administrator, as specified in Equation 1:

$$\text{If } T_i(t) < \tau, \text{ then: } \begin{cases} \text{Revoke access to } D_i, \\ \text{Log event on-chain,} \\ \text{Notify administrator.} \end{cases} \tag{1}$$

To maintain data integrity, the blockchain employs a consensus mechanism that ensures that all updates are validated and recorded consistently. The new ledger state L_t is computed as a function of the previous state L_{t-1} and the new data block Δ_t, as $L_t = \text{Consensus}(L_{t-1}, \Delta_t)$. This block includes updated trust scores and any policy enforcement actions taken at that time. Together, these components create a decentralized, intelligent, and adaptive framework for trust management in IIoT environments. The model leverages a custom blockchain protocol, called PureChain, to provide secure and automated policy enforcement according to the ZT principles.

B. Zero Trust Phase

In the ZT phase, access decisions are governed by a binary function that considers multiple security factors before granting or denying access. Specifically, access control relies on the evaluation in Equation 2.

$$A(u, d, r, t) = \begin{cases} 1, & \text{if } P(u, d, r, C_t) = 1 \text{ and } M(u) = 1, \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

where $A(u, d, r, t)$ represents the access decision at time t for 1 = allow, 0 = deny. u is the user access request, d is device used in the request, r is the requested resource. C_t depicts the contextual data at time t (e.g. location, usage pattern, history), $P(u, d, r, C_t)$ is the policy function returning 1 if the request complies with access control rules, and $M(u)$ is the multi-factor authentication function (1 if verified, 0 if not).

C. Blockchain Phase

In the blockchain phase of the system, each device d is continuously evaluated and assigned a dynamic trust score $T_d(t) \in [0, 1]$, which reflects the behavior of the device over time. This score evolves based on real-time input from an anomaly detection engine. The update rule is defined as $T_d(t+1) = \alpha \cdot T_d(t) - \beta \cdot A_d(t)$, where $T_d(t)$ is the trust score of the device d at time t, $A_d(t)$ is the anomaly score (1 = anomaly, 0 = normal). $\alpha \in (0, 1)$ represent the trust retention coefficient and $\beta > 0$ is the penalty coefficient. The access is automatically revoked if the updated trust score falls below a threshold $\theta \in [0, 1]$. All events, including access requests, anomaly alerts, and changes in trust score, are permanently recorded on the blockchain to ensure transparency and accountability. This as $T_i = \text{Hash}(T_{i-1} + \text{Event Data}_i + \text{Timestamp}_i)$. Each new transaction is cryptographically linked to the previous one, forming an immutable ledger. The structure of each block is defined in Equation 3.

$$H(B_n) = H(B_{n-1}) + \sum_{i=1}^{m} H(T_i) \tag{3}$$

where $H(B_n)$ represents the hash of the current block, $H(B_{n-1})$ is the hash of the previous block, $H(T_i)$ is the hash of transaction i and m is the number of transactions in the block. To maintain low-latency blockchain consistency, the system utilizes the PoA^2 consensus, which combines Proof of Authority with association-based validation. Smart contracts autonomously enforce security policies, triggering actions as per Equation 4 when a device violates rules or its trust score falls below θ.

$$SC(x) = \begin{cases} 1, & \text{if } x \text{ violates policy or } T_d(t) < \theta \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

D. AI-Driven Phase

The LSTM-based anomaly detection model is designed to process time-series data by capturing both short-term and long-term dependencies through memory cells. Each memory cell maintains two critical components: a cell state C_t holds long-term memory and a hidden state h_t provides output for the current time step. Information flow within the LSTM is regulated by three types of gates: the forget gate f_t controls how much of the previous cell state is retained. The input gate i_t and the candidate cell state $\tilde{C}_t$ determine the new information to add to the memory. The updated cell state is expressed as $C_t = f_t \odot C_{t-1} + i_t \odot \tilde{C}_t$, the output gate o_t decides which part of the cell state C_t is passed to the hidden state h_t. The final hidden state h_t is used to make predictions using the softmax function as $\hat{y} = \text{softmax}(W_y h_t + b_y)$, when an anomaly is flagged, the detection is expressed by Equation 5:

$$\hat{y}_t = \begin{cases} 1, & \text{if score}(x_t) > \theta \\ 0, & \text{otherwise} \end{cases} \tag{5}$$

Here, $\hat{y}_t$ represents the predicted label at time t, score(x_t) is the anomaly score for input x_t, and θ is a predefined threshold. A value of 1 indicates an anomaly, while 0 indicates normal behavior.

IV. Performance Assessment and Discussion

A. Dataset Description

This study evaluates the proposed PoA^2 framework using two benchmark datasets: WUSTL-IIoT-2021 [19] and IoTForge Pro [20]. WUSTL-IIoT-2021 includes over 1.19 million labeled IIoT flows across 41 features, with a class imbalance favoring normal (92%) over primarily DoS attack traffic (7%). Preprocessing involved min-max normalization and linear interpolation (Equation 6) to address scaling and missing values.

$$x' = \frac{x - x_{\min}}{x_{\max} - x_{\min}}. \tag{6}$$

IoTForge Pro offers a comprehensive evaluation environment for IIoT security, encompassing a diverse range of synthetic and real-world attack types, including ransomware, XSS, and password attacks, alongside regular traffic. Experiments were conducted in Python on Google Colab using a 6th-generation Intel i5-6300U CPU with 4 GB of RAM (Windows 11). Blockchain operations were simulated via a custom Python class that appended encrypted client data as blocks.

B. Model Performance

Figure 3 compares the performance of BiLSTM, LSTM, and CNN models on two IIoT datasets. In IoTForge Pro, all models perform exceptionally, with metrics above 99.7%. CNN leads slightly in precision and F1-score, showing strong detection with low false alarms. On the WUSTL-IIoT-2021 dataset, which is more challenging, LSTM performs best with a precision of 97.8% and F1-score of 96.4%, followed by BiLSTM. CNN shows the weakest performance, especially in recall. Thus, LSTM proves to be the most robust and adaptable model, making it the best overall anomaly detection model in both environments.

TABLE I: Training and Inference Times

	IoTForge Pro		WUSTL-IIoT-2021	
	Training Time (s)	Inference Time (s)	Training Time (s)	Inference Time (s)
BiLSTM	10876.0	0.000695	873.99	222.64
LSTM	6276.0	0.000424	727.30	20.28
CNN	1070.0	0.000102	1287.89	20.75

Table I shows that CNN trains fastest on IoTForge Pro (1070.0s) and has the lowest inference time (0.000102s), making it ideal for real-time use. BiLSTM trains the slowest (10876.0s) but still maintains low inference time, while LSTM

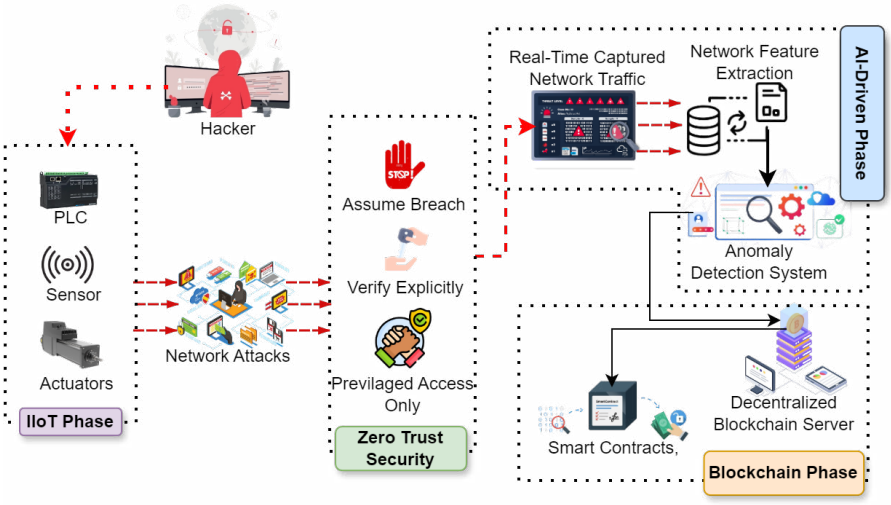
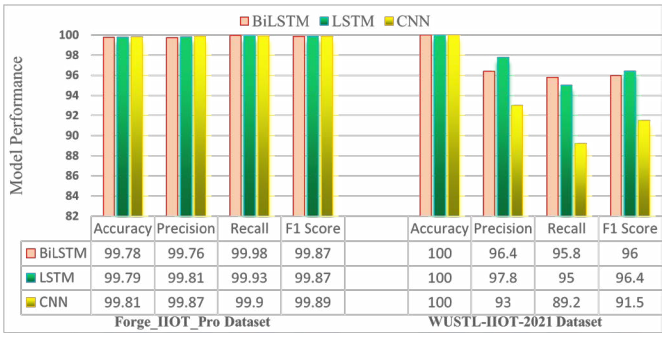


Fig. 2: The architecture of proposed AI-driven anomaly detection for IIoT.



	Accuracy	Precision	Recall	F1 Score	Accuracy	Precision	Recall	F1 Score
BiLSTM	99.78	99.76	99.98	99.87	100	96.4	95.8	96
LSTM	99.79	99.81	99.93	99.87	100	97.8	95	96.4
CNN	99.81	99.87	99.9	99.89	100	93	89.2	91.5

Fig. 3: Performance Analysis.

offers a good balance. On WUSTL-IIoT-2021, LSTM trains fastest (727.30s) and has the shortest inference time (20.28s), outperforming CNN and BiLSTM. BiLSTM has the highest inference time (222.64s), making it less suitable for latency-sensitive scenarios. Hence, LSTM offers the best trade-off between training and inference time, confirming its practicality for real-time IIoT anomaly detection.

C. The Blockchain Evaluation

TABLE II: Blockchain Platform Metrics across Datasets

Dataset	Platform	Throughput	Latency	Energy	Scalability
IoTForge Pro	Ethereum	5.00	0.1997	1520.65	0.5628
	Hyperledger	9.94	0.1005	30.48	0.7875
	PureChain	16.82	0.0594	12.43	0.8613
WUSTL-IIoT-2021	Ethereum	4.98	0.2010	14.99	0.5748
	Hyperledger	10.02	0.0998	298.02	0.7561
	PureChain	16.64	0.0601	124.60	0.8854

Table II shows that PureChain outperforms Ethereum and Hyperledger across all key metrics. It achieves the highest throughput (over 16 TPS), the lowest latency (around 0.06s), and strong energy efficiency, especially on the IoTForge Pro dataset. Hyperledger ranks second in most areas, while Ethereum consistently lags with the lowest throughput, highest latency, and inconsistent energy use. PureChain also shows the best scalability on both datasets. These results highlight PureChain as the most efficient and scalable blockchain platform for IIoT security applications.

TABLE III: Consensus Mechanism Metrics across Datasets

Dataset	Consensus	Throughput	Latency	Energy	Scalability
IoTForge Pro	PoA	4.94	0.2100	15.95	1.01
	PoS	8.45	0.3415	60.76	0.82
	PoW	2.90	2.8697	195.95	0.57
	PoA^2	7.61	0.08612	5.14	1.47
WUSTL-IIoT-2021	PoA	4.03	0.1626	10.79	1.19
	PoS	9.30	0.3623	62.26	0.84
	PoW	3.14	1.2023	151.19	0.58
	PoA^2	6.71	0.0552	5.84	1.45

Table III shows that PoA^2 outperforms PoA, PoS, and PoW across key metrics. While PoS achieves the highest throughput, PoA^2 offers the best overall balance, delivering the lowest latency (0.0552s), the highest scalability (1.45), and the lowest energy consumption (5.84 kWh). It also maintains strong throughput (6.71 TPS), making it suitable for resource-constrained IIoT environments in real time. These results position PoA^2 as the most efficient and scalable consensus mechanism for secure integration of IIoT blockchains.

D. The ZTA Evaluation

TABLE IV: Zero Trust Security Model Metrics

Metric	IoTForge Pro	WUSTL-IIoT-2021
Accuracy (%)	98.69	98.46
Latency (s)	0.42	0.31
Detection Time (s)	0.22	0.25
Resource Utilization (%)	84.68	76.99

Table IV shows that the ZT model performs effectively on both IoTForge Pro and WUSTL-IIoT-2021 datasets. Accuracy is high for both (98.69% and 98.46%, respectively), demonstrating strong generalizability. WUSTL-IIoT-2021 has slightly lower latency (0.31s), indicating a faster system response, while IoTForge Pro detects anomalies slightly quicker (0.22s).

However, IoTForge Pro consumes more resources (84.68%) compared to WUSTL-IIoT-2021 (76.99%). Overall, IoTForge Pro offers slightly better detection, but WUSTL-IIoT-2021 is more resource-efficient. Table V shows the comparative analysis that shows that the proposed model outperforms the prior threat detection approaches in all key metrics. Although some existing models such as [13], [14], [16] deliver high accuracy above 96%, they lack real-time capability and full AI integration. The proposed model delivers the highest accuracy 99.79%, precision 99.83%, and F1-score 99.87%, while also supporting real-time detection and complete AI integration.

TABLE V: Performance comparison of threat detection

Ref.	Accuracy (%)	Precision (%)	F1-Score (%)	Real-Time Support	AI Integration
[12]	94.76	94.85	94.76	No	No
[13]	96.88	96.31	96.58	Partial	No
[14]	96.92	96.89	96.92	No	No
[16]	96.98	96.13	96.44	No	Partial
Proposed	**99.79**	**99.81**	**99.87**	**Yes**	**Yes**

E. Finding and Implications

PureChain outperforms Ethereum and Hyperledger in terms of throughput, latency, and energy efficiency across various datasets. The PoA^2 consensus achieves the best balance among mechanisms, offering high scalability, low energy use, and fast response compared to PoW, PoS, and PoA. The LSTM-based anomaly detection model delivers the highest accuracy, especially on the WUSTL-IIoT-2021 dataset, while maintaining efficient training and inference. The ZT model also performs well in constrained environments. Together, PoA^2 and PureChain form a scalable, secure, and energy-efficient foundation for real-time IIoT cybersecurity, integrating decentralized trust, Zero Trust enforcement, and AI-driven anomaly detection.

V. Conclusion

This study presents PureChain, a blockchain-integrating Zero Trust framework to enhance the security of Industrial IoT. Utilizing a custom PoA^2 consensus mechanism, PureChain overcomes the limitations of traditional blockchain systems by improving throughput, latency, scalability, and energy efficiency. The integration of an LSTM-based anomaly detection engine enables the accurate identification of real-time threats. Experimental results on the WUSTL-IIoT-2021 and IoTForge Pro datasets confirm PureChain's superior detection accuracy, responsiveness, and resource efficiency. Overall, the synergy of blockchain, ZT, and AI in PureChain offers a robust, scalable, and practical solution for securing complex IIoT infrastructures in real-world deployments.

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] K. Gai, M. Qiu, and X. Zhao, "Secure Cloud Computing: Combining Zero Trust with Blockchain for the Internet of Things," *Journal of Cloud Computing: Advances, Systems, and Applications*, vol. 12, no. 1, pp. 13–23, 2023.

[2] A. Arora and S. Sharma, "Blockchain-Based Zero Trust Architecture: An Emerging Paradigm in Network Security," *International Journal of Network Security*, vol. 21, no. 1, pp. 42–58, 2023.

[3] Z. H. Khan, V. C. Leung, and H. Song, "Enhancing Industrial IoT Security Using Zero Trust and Blockchain," *Security and Privacy*, vol. 5, no. 3, p. e204, 2022.

[4] Q. Zhang, M. Yu, and J. Wang, "An Efficient Integration of Blockchain with Zero Trust in Cloud-Based IoT Networks," *Future Internet*, vol. 15, no. 8, p. 274, 2023.

[5] W. Chen, Y. Zhang, and L. Li, "A Survey on Zero Trust Architecture in Cloud and IoT Security," *IEEE Access*, vol. 11, pp. 22 874–22 887, 2023.

[6] T. Mei, K. Gai, and W. Xiong, "The Role of Zero Trust Architecture in Securing Smart Cities," *International Journal of Smart Cities and Artificial Intelligence*, vol. 7, no. 1, pp. 58–71, 2024.

[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, 2024.

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

[9] B. Rai and R. Pundir, "Blockchain-Enhanced Security: Bridging Zero Trust Architecture and Industrial IoT," *Journal of Industrial Information Integration*, vol. 27, p. 100317, 2023.

[10] 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 *2025 IEEE International Conference on Consumer Electronics (ICCE)*, 2025, pp. 1–6.

[11] L. A. C. Ahakonye, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Agnostic CH-DT Technique for SCADA Network High-Dimensional Data-Aware Intrusion Detection System," *IEEE Internet of Things Journal*, vol. 10, no. 12, pp. 10 344–10 356, 2023.

[12] S. M. Awan, M. A. Azad, J. Arshad, U. Waheed, and T. Sharif, "A Blockchain-Inspired Attribute-Based Zero-Trust Access Control Model for IoT," *Information*, vol. 14, no. 2, p. 129, 2023.

[13] S. Li, M. Iqbal, and N. Saxena, "Future Industry Internet of Things with Zero-Trust Security," *Information Systems Frontiers*, vol. 26, no. 5, pp. 1653–1666, 2024.

[14] S. Nie, J. Ren, R. Wu, P. Han, Z. Han, and W. Wan, "Zero-Trust Access Control Mechanism Based on Blockchain and Inner-Product Encryption in the Internet of Things in a 6G Environment," *Sensors*, vol. 25, no. 2, p. 550, 2025.

[15] Y. Bobde, G. Narayanan, M. Jati, R. S. P. Raj, I. Cvitić, and D. Peraković, "Enhancing Industrial IoT Network Security Through Blockchain Integration," *Electronics*, vol. 13, no. 4, p. 687, 2024.

[16] A. Nazir, J. He, N. Zhu, A. Wajahat, F. Ullah, S. Qureshi, X. Ma, and M. S. Pathan, "Collaborative Threat Intelligence: Enhancing IoT Security Through Blockchain and Machine Learning Integration," *Journal of King Saud University-Computer and Information Sciences*, vol. 36, no. 2, p. 101939, 2024.

[17] A. Verma, P. Bhattacharya, N. Madhani, C. Trivedi, B. Bhushan, S. Tanwar, G. Sharma, P. N. Bokoro, and R. Sharma, "Blockchain for Industry 5.0: Vision, Opportunities, Key Enablers, and Future Directions," *IEEE Access*, vol. 10, pp. 69 160–69 199, 2022.

[18] U. A. Bukar, H. Ibrahim, and B. S. Yahaya, "Charting the future of ai in the next decade: Emerging trends and conclusions," *The Smart Life Revolution: Embracing AI and IoT in Society*, p. 245, 2025.

[19] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "WUSTL-IIoT-2021 Dataset for IIoT Cybersecurity Research," October 2021.

[20] 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.