BLIND-Twin: Blockchain-Assisted LLM-Based CDS for Digital Twin-Enhanced Industrial AIoT

Mohtasin Golam, Md Mahinur Alam, Md Raihan Subhan, Dong-Seong Kim, and Jae-Min Lee
Networked Systems Laboratory, Department of IT Convergence Engineering,
Kumoh National Institute of Technology, Gumi, South Korea.
(golam248, mahinuralam213, raihan, dskim, and ljmpaul)@kumoh.ac.kr

***Abstract*—The interconnected and diverse nature of Digital Twin (DT)-based industrial Artificial Internet of Things (AIoT) systems exposes them to potential cyber threats and malicious activities. This paper introduces a novel framework called BLIND-Twin, which leverages blockchain, DT, and Large Language Model (LLM) technologies to address critical security and scalability challenges in industrial AIoT networks. By integrating DT technology, BLIND-Twin continuously mirrors physical environments, enabling real-time monitoring and synthetic data generation to simulate diverse threat scenarios. Data from the DT undergoes feature extraction via a Long Short-Term Memory (LSTM) Autoencoder (LSTM-AE) to extract essential temporal patterns, while the LLM enables adaptive, context-aware intrusion detection without retraining. A permissioned blockchain layer ensures data integrity, privacy, and secure logging through smart contracts, supporting automated threat response with verifiable audit trails. The framework's decentralized architecture mitigates Single Points of Failure (SPoF), addressing scalability and privacy concerns. Performance evaluations utilizing datasets like 5G-NIDD and CICIoT2023 demonstrate BLIND-Twin's capability in accurately detecting various cyber threats by achieving 99.63% accuracy with minimal latency, showcasing its effectiveness for complex industrial AIoT environments.**

***Index Terms*—Artificial Internet of Things (AIoT), Blockchain, Digital Twin (DT), Federated Learning (FL), and Unmanned Aerial Vehicle (UAV).**

I. Introduction

The Internet of Things (IoT) is essential for industry, facilitating smart sensing and multiple device connections. The extensive generation of sensitive data presents new privacy and security challenges. Artificial Intelligence of Things (AIoT) is a promising development in this domain, which integrates AI into IoT systems to enhance operational efficiency through intelligent processing and automation [1]. However, the limited computational capacity of many IoT devices complicates this integration and makes it challenging to utilize AI's potential for performance improvement. Moreover, AIoT ecosystems face additional cybersecurity risks, such as intrusion attacks, on-path attacks and network congestion, which can compromise data aggregation and disrupt operations [1]. Innovations in network architecture and security protocols are needed to ensure resilience and effectiveness amidst emerging cyber threats.

Digital Twin (DT) has recently emerged as a transformative concept, gaining significant industrial attention. A DT represents a physical entity's virtual replica, continuously mirroring its real-world counterpart's state and behaviour through bidirectional synchronization, enabling seamless interaction between virtual and physical environments [5]. By offloading computational tasks to the virtual model, DTs alleviate the processing burden on resource-constrained physical devices, enhancing system efficiency and reducing latency [6]. However, despite its advantages, DT systems' increased connectivity and integration introduce cybersecurity vulnerabilities. Unauthorized intrusions, data breaches, or manipulation attacks could compromise the accuracy and integrity of both the digital and physical components, leading to potential disruptions or safety risks [7].

Intrusion detection systems (IDS) leveraging machine learning (ML) and deep learning (DL) have been deployed for identifying cyber threats in IIoT environments [8]. However, these models remain susceptible to data poisoning attacks, where compromised data degrades the accuracy and reliability of detection mechanisms. Centralized learning approaches in these systems often encounter critical challenges, including high communication overhead, data privacy, and scalability bottlenecks due to the need to aggregate large-scale data at a central server. Using Large Language Models (LLMs) could enhance cyber threat detection in AIoT by enabling localized, context-aware detection and mitigating communication, privacy, and scalability challenges [9]. LLMs enable real-time threat detection at the edge, reducing the need for data transmission to centralized servers [10]. Their advanced contextual understanding enhances detection accuracy, even with minimal data, reducing the dependency on large-scale data aggregation. Furthermore, LLMs provide adaptive learning capabilities, enabling them to operate effectively in dynamic environments without extensive re-training [11], ensuring scalable security across expanding AIoT networks.

Blockchain functions as a distributed ledger, where each participant holds a synchronized copy, ensuring that any modification is validated by the network, thus preventing unauthorized changes [12]. Combining blockchain's immutable, decentralized properties with AI-powered detection enables a secure and reliable framework for distributed DT-based intrusion detection [13], ensuring trustworthy, real-time identification and mitigation of cyberattacks in industrial AIoT networks. Conventional IDS methods [2] [3] [4] face significant limitations when applied to cyber threat detection in Digital Twin (DT) environments. DT-based IIoT ecosystems produce vast volumes of data, which traditional IDS solutions

ICC 2025 - IEEE International Conference on Communications | 979-8-3315-0521-9/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICC52391.2025.11161313

TABLE I: Comparison between Proposed System and Existing CDS Framework for DT-based IoT Networks

Ref.	Target System	Dataset	CA	PM	SA	DV	MT	Accuracy (%)
[2]	DT-based Healthcare	CICDDoS2019 dataset	×	×	✓	✓	✓	98.77
[3]	Digital Twin IIoT Network	CICIDS-2017 and ToN-IoT	✓	×	✓	✓	✓	99.14
[4]	DT-based Smart Grid System	LCL dataset	✓	✓	✓	✓	✓	N/A
BLIND-Twin	DT-based Industial AIoT	5G-NIDD and CICIoT2023	✓	✓	✓	✓	✓	99.53

* CA - Context Awareness, * PM - Predictive Maintenance, * SA - Situational Awareness, * DV - Data Verifiability, * MT - Model Trustworthiness, ✓ - Considered, × - Non-Considered

may not process or analyze effectively for real-time threat detection. Moreover, these environments present a broader and more complex attack surface, as cyber attackers can exploit vulnerabilities in both the physical systems and their digital counterparts. Table I highlights recent approaches compared to the proposed BLIND-Twin system, which introduces key features highlighted in the table. Given the necessity for a data privacy, scalability, and efficient CDS model tailored for DT-based AIoT networks, this study introduced an innovative framework named BLIND-Twin that comprehensively addresses these specific challenges. The major contributions of this paper are illustrated below:

- Proposed a novel BLIND-Twin framework that leverages blockchain's immutable and decentralized properties within a DT environment, providing data-verifiable security, transparency, and tamper-resistant logging for industrial AIoT networks.
- The framework combines an LSTM autoencoder for feature extraction with a context-aware LLM, enabling adaptive and accurate intrusion detection without retraining in complex, real-time industrial settings.
- BLIND-Twin employs DT technology for real-time monitoring and synthetic threat generation, supports privacy-preserving intrusion detection, and scales efficiently across diverse and evolving industrial AIoT network applications.

II. Proposed Framework

A. Problem Formulation

Existing cyber-threat detection systems (CDS) in industrial AIoT and DT-based networks struggle to balance scalability, privacy, and real-time detection. Traditional CDS frameworks relying on centralized DL approaches are often plagued by communication overhead, data privacy risks, and limited scalability, making them unsuitable for complex DT-enabled industrial systems. While federated learning (FL) has been introduced to address some of these limitations by decentralizing the training process, its dependency on a central aggregation coordinator introduces a single point of failure (SPoF) and leaves it susceptible to malicious aggregator attacks. Blockchain integration into FL frameworks offers promising solutions, such as secure, immutable data exchange and resistance to data poisoning attacks. However, current blockchain-FL combinations suffer from high transaction times, which limit their ability to support real-time CDS deployment. Additionally, these frameworks often overlook the complex, evolving interactions between physical and virtual layers within DT ecosystems, creating gaps in CDS.

B. Proposed BLIND-Twin framework

The proposed BLIND-Twin architecture integrates DT, Blockchain, and LLM technologies to develop robust and adaptable CIDS for industrial AIoT networks. Real-time data is collected from industrial sensors at the physical layer, capturing operational variables and network activity in critical infrastructure environments. This data is synchronized with the DT layer, where the DT replicates actual conditions, enabling real-time simulations and generating synthetic threat scenarios. Feature extraction via an autoencoder with long short-term memory (LSTM-AE) processes both actual and synthetic data to identify critical temporal patterns, following that analyzed by the LLM for threat detection. The LLM adjusts to emerging threats without retraining through context-aware learning, improving context-aware cyber threat detection and response capabilities [9]. The proposed system, illustrated in Fig. 1, comprises three layers (physical, network, and DT application layers). A permissioned blockchain ensures data integrity and controls access in the on-chain network layer. It employs smart contracts to validate detected threats and automate response actions while immutably logging events for enhanced security and auditability. By merging the LLM's contextual learning with blockchain's decentralized, tamper-resistant storage, BLIND-Twin provides a scalable and secure defence system tailored for dynamic industrial environments. This workflow enables continuous learning and adaptability, establishing BLIND-Twin as an effective and robust solution against emerging cyber threats in complex and dynamic operating industrial environments.

C. LLM-based Cyber Threat Detection Model

1) LSTM-AE Based Feature Extraction Technique: The LSTM-AE model integrates LSTM networks with autoencoders to extract features from data effectively. It functions as a sparsity-constrained autoencoder, using LSTM's capacity to identify temporal relationships and extract pertinent patterns from sequential data. Assuming an industrial AIoT setup with UAV and IoT sensors $\mathfrak{s}$ collecting data samples $\mathfrak{D}_{\mathfrak{s}}$, the input data matrix is denoted by $\imath = [\imath_1, \imath_2, ..., \imath_{\mathfrak{s}}] \in \mathbb{R}^{\mathfrak{D}_{\mathfrak{s}}} \times \mathfrak{s}$. Using the LSTM-AE-based feature extraction method, the hidden layer's output matrix is expressed as $\infty = [\infty_1^*, \infty_1^*, ..., \infty_{\mathfrak{s}}^*] \in \mathbb{R}^{\mathfrak{s}} \times \delta$, where δ is the feature vector dimensionality in the hidden layer. The structure captures crucial temporal patterns

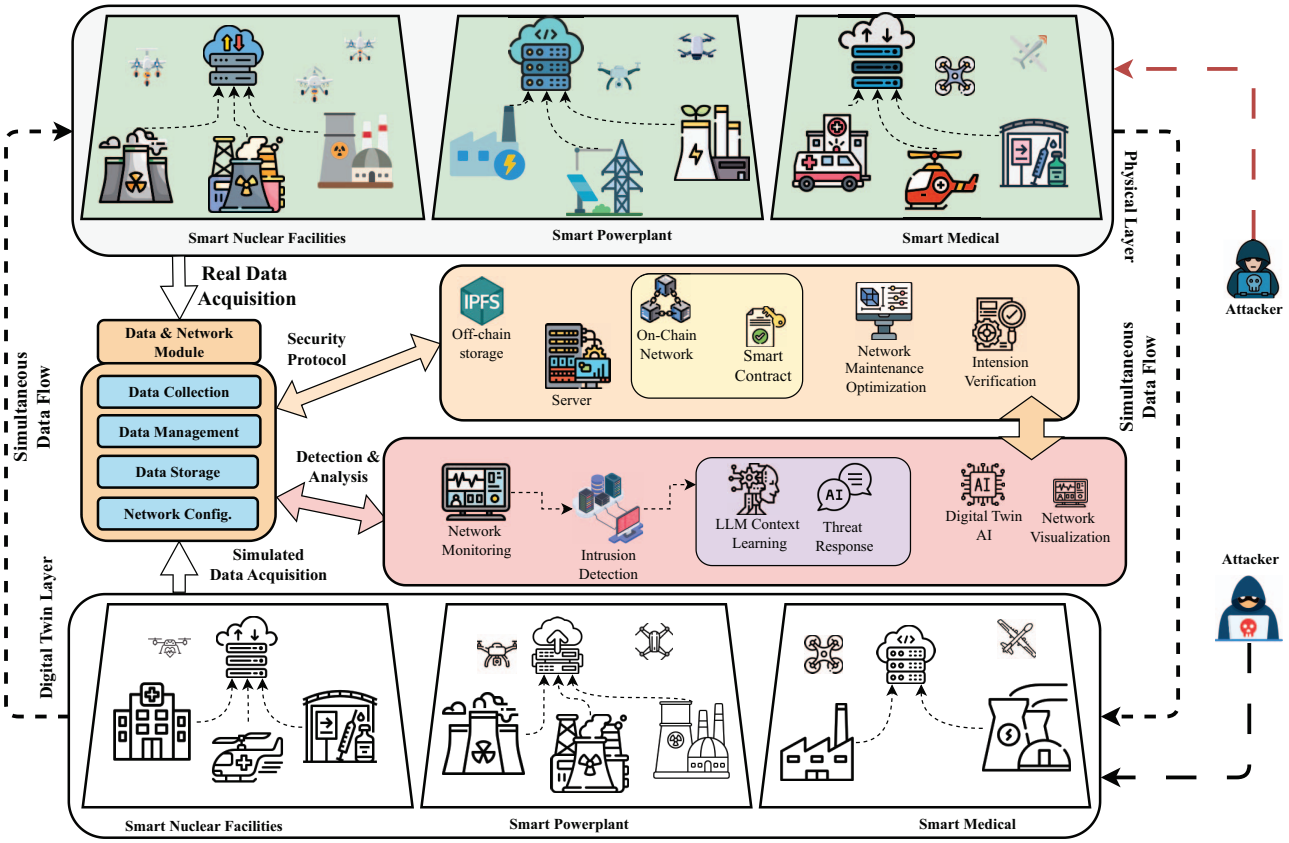

Fig. 1: Proposed Blockchain-Assisted LLM-Based CDS for DT-Based AIoT Networks

in sensor data, enhancing accuracy in tasks like intrusion detection.

2) LSTM AutoEncoder (LSTM-AE): The LSTM-AE employs an encoder-decoder structure with LSTM cells to capture essential temporal features from industrial $\mathfrak{D}_{\mathfrak{s}}$. The encoder transforms the input $\imath$, into a lower-dimensional latent representation $\imath'$ using the formula $\imath' = \mathring{A}(\omega_e \imath + \beta_e)$, while the decoder reconstructs $\imath$ from $\imath'$ through $\imath^{\circ} = \mathring{A}(\omega_d \imath' + \beta_d)$. Here, ω_e and ω_d are the weights β_e β_d, and $\mathring{A}(.)$ represents the activation function, reducing dimensionality and ensuring efficient feature extraction for the LLM-based CDS. The optimization objective for training the LSTM-AE minimizes the reconstruction error between $\imath$ and $\imath^{\circ}$ through learning the model parameters ω, β by reducing the following objective:

$$\{\omega^{\circ} + \imath'\} = \partial_{min_{(\omega^{\circ}, \imath')}} \left\{ \frac{1}{2\mathfrak{n}_{\mathfrak{s}}} \sum_{i=1}^{\mathfrak{n}_{\mathfrak{s}}} l(\imath_i, \hat{\imath}_i) + \frac{\lambda}{2} \sum_{\Re=1}^{2} \|\omega_{\Re}\|_{\mathfrak{F}}^2 \right\} \tag{1}$$

Here, $l(.)$ denotes the reconstruction loss for $\mathfrak{s}$, $\mathfrak{n}_{\mathfrak{s}}$ is the number of samples, and λ is a regularization parameter applied to control overfitting through weight regularization. This concise formulation captures the objective function's essential elements by minimizing the reconstruction error across samples while applying Frobenius norm regularization $\|\omega_{\Re}\|_{\mathfrak{F}}^2$. The Kullback-Leibler divergence (KLD) functions as a sparsity constraint in the stacked AE, improving the model's capacity to identify essential features by controlling neuron activations. The KLD is calculated as follows:

$$\sum_{z=1}^{m} \mathrm{KLD}(\varrho \,||\, \hat{\varrho}_z) = \sum_{z=1}^{m} \left\{ (1-\varrho) \log \frac{1-\varrho}{1-\hat{\varrho}_z} + \varrho \log \frac{\varrho}{\hat{\varrho}_J} \right\} \tag{2}$$

Here, the sparsity parameter ϱ sets the desired activation level for each neuron, with $\hat{\varrho}_z$ representing the average activation for neuron z across training samples. In the BAFL-LLM framework, the LSTM handles encoding and decoding, capturing temporal dependencies, as shown in Fig. 2. LSTM-AE focuses on important data features by limiting the latent space to fewer dimensions than the input. This improves anomaly detection and the model's ability to find important patterns for intrusion detection.

3) Context-Aware Learning for LLM: In addressing network intrusion detection challenges, context-aware learning is an effective approach for tailoring pre-trained LLM to be task-specific without modifying their fundamental features. This method integrates applicable text-based examples with prompts, altering the input format to obtain the desired re-

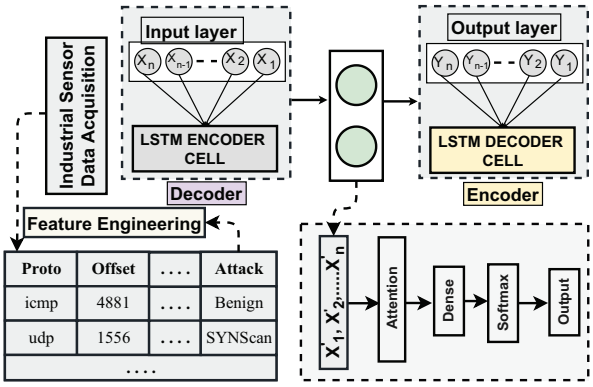

Fig. 2: LSTM-AE Based Feature Extraction for LLM Model

sponse. This method can be represented as:

$$\mathfrak{o}_{\mathfrak{t}}^{*} = \partial_{max}\rho\left(\mathfrak{o}_{\mathfrak{t}} \mid \mathfrak{c}_{\mathfrak{t}}, \{(\mathfrak{c}_{\mathfrak{i}}, \mathfrak{o}_{\mathfrak{i}})\}_{i=1}^{n}; \Phi_{pre}\right) \tag{2}$$

In this context, $\mathfrak{o}_{\mathfrak{t}}^{*}$ represents the LLM's output for a network intrusion detection task, while $\rho(...)$ reflects the probability of generating this output. ∂_{max} emphasizes that we are finding the value of $\mathfrak{o}_{\mathfrak{t}}$ that maximizes the probability. Here, $\mathfrak{o}_{\mathfrak{t}}$ indicates the current network conditions and $(\mathfrak{c}_{\mathfrak{i}}, \mathfrak{o}_{\mathfrak{i}})$ denotes the n-th example provided as context for guiding the model. The term Φ_{pre} represents the parameters of the pre-trained LLM. By leveraging these contextual examples, the configuration leads the LLM towards producing consistent and accurate outputs, aligning with the task's requirements. This approach is particularly advantageous for network intrusion detection.

D. Prompting and Decision Extraction

Once data is preprocessed, the BLIND-Twin framework constructs specific prompts to guide the LLM in network security monitoring. These prompts are meticulously structured, starting with clear instructions that define network intrusion detection in a DT-enabled industrial AIoT environment and establishing the LLM's role. Task-specific examples derived from benign and malicious traffic patterns are included to enable the LLM to distinguish between normal and abnormal activities. Additionally, prompts are crafted with explicit output formatting, ensuring that the LLM's responses are clear and actionable for intrusion detection. Following the LLM's analysis, decisions are extracted to activate automated response protocols via blockchain-based smart contracts. For instance, if an anomaly is detected, the system can isolate compromised devices, redirect communications, or initiate defence mechanisms. Each decision is securely recorded on the blockchain, providing an immutable audit trail for accountability and transparency, enhancing the framework's robustness in effectively handling industrial cyber threats.

III. Performance Analysis of the BLIND-Twin

A. Dataset Description

The BLIND-Twin framework employs two distinct datasets, each meticulously designed to encapsulate certain attack types and data characteristics.

- 5G-NIDD: The 5G-NIDD dataset [14] was derived from a fully operational 5G test network, and it encompasses two primary types of attacks: Denial of Service (DoS) and port scans. The DoS category features multiple forms, such as ICMP flood, UDP flood, SYN flood, HTTP flood, and Slow-rate DoS. Additionally, the dataset includes three distinct port scan techniques: SYN scan, TCP connect scan, and UDP scan, providing a diverse set of attack vectors for robust IDS evaluation.
- CICIoT2023: The CICIoT2023 [15] dataset represents a realistic IoT attack dataset created using a comprehensive network topology with 105 IoT devices configured as both attackers and victims. To develop this dataset, 33 distinct attacks were executed across the IoT network, specifically structured into 7 attack classes. Features are grouped in 10-packet windows for certain attack types, including Backdoor Malware, Browser Hijacking, and SQL Injection. DDoS methods, including SYN Flood, HTTP Flood, and Mirai-based attack features, are collected in 100-packet windows for high-impact attacks.

B. LLM-Based Cyber Threats Detection Performance

Table II provides a comparative analysis of the performance of different intrusion detection models applied to the CICIoT and 5G-NIDD datasets, emphasizing key evaluation metrics such as accuracy, precision, recall, F1-score, loss, and Area Under the Curve (AUC). The suggested BLIND-Twin model consistently exhibits exceptional performance across both datasets, attaining the highest accuracy (99.42% on CICIoT and 99.63% on 5G-NIDD), along with a high AUC of 0.996 and 0.997, respectively, signifying robust classification proficiency. Significantly, BLIND-Twin exhibits reduced loss values (0.041 for CICIoT and 0.034 for 5G-NIDD), demonstrating its efficacy and resilience in reducing classification inaccuracies. While achieving relatively high performance, other models lag behind BLIND-Twin, particularly in precision, recall, and F1-score, which are slightly lower across both datasets. The comparison emphasizes BLIND-Twin's effectiveness in precisely identifying intrusions with low error, showcasing its versatility in diverse industrial AIoT scenarios and its superiority over existing models by attaining optimal detection metrics across multiple datasets.

Table III presents a comparative analysis of SecurityBERT [10], DistilBERT [11], and the proposed BLIND-Twin model in terms of their architectural features and computational requirements, tailored for different types of training data. SecurityBERT features a 768-dimensional embedding and a 12-layer encoder, with a considerable intermediate layer size of 3072 and a high parameter count of 110M, resulting in substantial memory demands (16 GB - 24 GB) and an inference speed of 400 ms per 128 tokens. DistilBERT, optimized for general-purpose text corpora, achieves a more streamlined design with a 512 embedding size, 6 encoder layers, and a reduced parameter count of 66M, leading to improved inference speed (200 ms per 128 tokens) and lower

TABLE II: Performance Comparison of Models on CICIoT and 5G-NIDD Datasets

Model	CICIoT Dataset						5G-NIDD Dataset					
	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Loss	AUC	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Loss	AUC
BLIND-Twin	99.42	98.89	98.16	98.02	0.041	0.996	99.63	98.27	98.54	98.40	0.034	0.997
[2]	98.89	98.42	97.66	97.54	0.048	0.993	98.77	97.69	97.32	97.50	0.055	0.992
[3]	98.91	97.53	98.74	97.63	0.046	0.994	99.02	97.81	97.98	97.89	0.044	0.995
[4]	98.68	97.12	96.98	97.05	0.058	0.990	98.57	97.05	96.93	96.99	0.060	0.989

TABLE III: Comparison of Model Features for Different Types of Training Data

Feature	SecurityBERT	DistilBERT	BLIND-Twin
Embedding Size	768	512	512
Number of Layers in Encoder	12	6	6
Number of Layers in Decoder	N/A	N/A	12
Size of Query, Key, Value	768	768	256
Intermediate Layer Size	3072	3072	768
Output Size of Transformer Layer	768	768	256
Input Token Length	512	512	128
Number of Parameters	110M	66M	57M
Training Memory Requirements	16 GB - 24 GB	6 GB - 12 GB	4 GB - 8 GB
Inference Speed	**400 ms per 128 tokens**	**200 ms per 128 tokens**	**150 ms per 128 tokens**

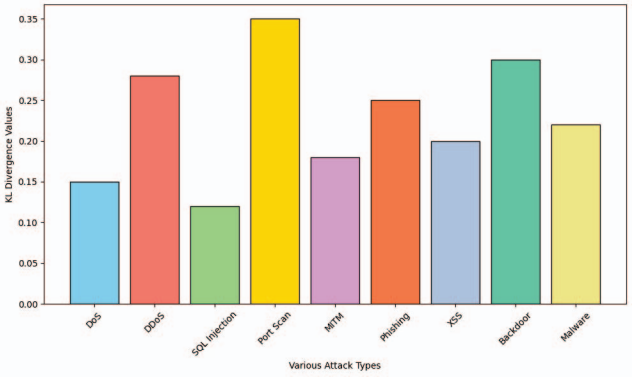

Fig. 3: KL Divergence values for generative synthetic attacks

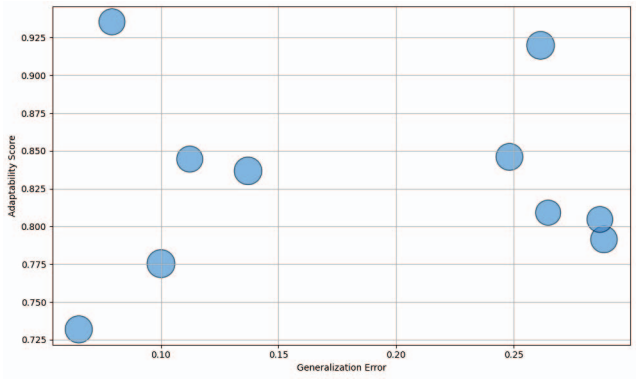

Fig. 4: Generalization Error and Adaptability Score in the BLIND-Twin Framework

memory requirements (6 GB - 12 GB). In contrast, BLIND-Twin, developed for industrial IoT and sensor network data, strikes a balance with a 512 embedding size, 6 encoder layers, and 12 decoder layers. Its smaller intermediate layer size (768) and optimized parameter count (57M) make it efficient, requiring only 4–8 GB of memory and achieving the fastest inference speed among the three (150 ms per 128 tokens). This comparison underscores BLIND-Twin's suitability for real-time, resource-constrained industrial environments, where computational efficiency and rapid response are critical.

C. Blockchain and DT Integrated BLIND-Twin Robustness and Adaptability Performance

The KLD values illustrated in Fig. 3 across different attack types offer a quantitative assessment of the model's accuracy in producing synthetic threat data corresponding to real-world distributions. Lower KLD values observed for attacks such as SQL Injection and DoS indicate a high level of generative accuracy. This suggests that the DT successfully replicates these attack types with minimal divergence from actual data patterns. In contrast, elevated KLD values, observed in Port Scan and Backdoor attacks, underscore the gaps where synthetic data does not adequately reflect the intricacies of real-world distributions, indicating opportunities for additional model improvement. This analysis highlights the effectiveness of simulating particular cyber-attack scenarios while also emulating specific areas for improvement. Using these insights, the BLIND-Twin framework can be refined to ensure that synthetic threat generation aligns closely with real-world threats, enhancing its reliability for training and validating IDS in DT-enabled AIoT networks.

Fig. 4 evaluates the framework's robustness and adaptability in handling real-world scenarios. A low Generalization Error indicates the model's ability to accurately identify unseen threats, reflecting its capability to extend beyond the limits of synthetic training data. Simultaneously, a high Adaptability Score demonstrates the framework's capacity for real-time updates, which is essential for maintaining relevance as new attack vectors emerge. Bubbles located in the upper-left quad-

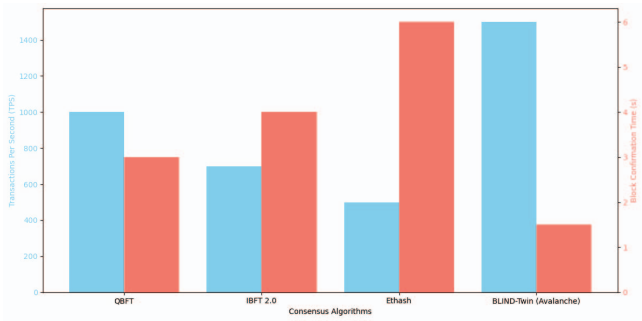

Fig. 5: Comparison of Throughput (TPS and Block Confirmation Time) Across Different Consensus Algorithms

rant signify an optimal balance, where the model generalizes effectively to unseen data and adapts efficiently to evolving threat landscapes, reinforcing BLIND-Twin's suitability for dynamic and high-stakes DT-enabled AIoT environments. This visualization underpins the framework's continuous learning capability, proving that BLIND-Twin can sustain high detection accuracy while adapting to complex, ever-changing cyber threat situations.

Fig. 5 illustrates the superior performance of the BLIND-Twin framework (using Avalanche consensus) in both Transactions Per Second (TPS) and Block Confirmation Time compared to other consensus algorithms. Its highest TPS is around 1500, which is above QBFT (1000 TPS), IBFT 2.0 (700 TPS), and Ethash (500 TPS). This illustrates the model's scalability and capacity to manage large amounts of real-time data. The minimum block confirmation time is 1.5 seconds, in contrast to QBFT (3 seconds), IBFT 2.0 (4 seconds), and Ethash (6 seconds). This reduced delay in block confirmation illustrates the capacity for swift and secure data logging, rendering it an optimal selection for low-latency, high-throughput blockchain integration in industrial systems.

IV. Conclusion

The BLIND-Twin framework integrates blockchain, DT, and LLM technologies to provide a scalable and secure intrusion detection solution for industrial AIoT networks. DT technology enables real-time system mirroring and synthetic threat simulations, strengthening the model's ability to anticipate and adapt to cyber threats. The framework enhances threat detection accuracy through LSTM-AE feature extraction and context-aware LLM analysis while maintaining adaptability without retraining. Blockchain's permissioned ledger ensures data integrity and automated responses, supporting a reliable, transparent threat management process. The decentralized architecture further addresses scalability and mitigates single points of failure, proving suitable for dynamic industrial environments. Performance assessments reveal that BLIND-Twin provides timely, accurate intrusion detection, validating its efficacy as a robust CDS for complex industrial applications. This work contributes a technically advanced, adaptable approach to safeguarding critical infrastructure in DT-enabled AIoT settings against evolving cyber threats.

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korean 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] J. Zhang and D. Tao, "Empowering things with intelligence: A survey of the progress, challenges, and opportunities in artificial intelligence of things," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 7789–7817, 2021.

[2] M. M. Salim, D. Camacho, and J. H. Park, "Digital twin and federated learning enabled cyberthreat detection system for iot networks," *Future Generation Computer Systems*, vol. 161, pp. 701–713, 2024.

[3] P. Kumar, R. Kumar, A. Kumar, A. A. Franklin, S. Garg, and S. Singh, "Blockchain and deep learning for secure communication in digital twin empowered industrial iot network," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 5, pp. 2802–2813, 2022.

[4] Y. Zhou, Y. Ge, and L. Jia, "Double robust federated digital twin modeling in smart grid," *IEEE Internet of Things Journal*, 2024.

[5] L. U. Khan, W. Saad, D. Niyato, Z. Han, and C. S. Hong, "Digital-twin-enabled 6g: Vision, architectural trends, and future directions," *IEEE Communications Magazine*, vol. 60, no. 1, pp. 74–80, 2022.

[6] H. Xu, J. Wu, Q. Pan, X. Guan, and M. Guizani, "A survey on digital twin for industrial internet of things: Applications, technologies and tools," *IEEE Communications Surveys & Tutorials*, 2023.

[7] R. Mustofa, M. Rafiquzzaman, and N. U. I. Hossain, "Analyzing the impact of cyber-attacks on the performance of digital twin-based industrial organizations," *Journal of Industrial Information Integration*, vol. 41, p. 100633, 2024.

[8] A. Zainudin, L. A. C. Ahakonye, R. Akter, D.-S. Kim, and J.-M. Lee, "An efficient hybrid-dnn for ddos detection and classification in software-defined iiot networks," *IEEE Internet of Things Journal*, vol. 10, no. 10, pp. 8491–8504, 2022.

[9] M. Golam, M. M. Alam, D.-S. Kim, and J.-M. Lee, "Blm-chain: Ai-driven blockchain for uav threat resistance in iobt," in *2024 15th International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2024, pp. 1609–1613.

[10] M. A. Ferrag, M. Ndhlovu, N. Tihanyi, L. C. Cordeiro, M. Debbah, T. Lestable, and N. S. Thandi, "Revolutionizing cyber threat detection with large language models: A privacy-preserving bert-based lightweight model for iot/iiot devices," *IEEE Access*, 2024.

[11] A. Diaf, A. A. Korba, N. E. Karabadji, and Y. Ghamri-Doudane, "Beyond detection: Leveraging large language models for cyber attack prediction in iot networks," in *2024 20th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*. IEEE, 2024, pp. 117–123.

[12] M. Golam, E. A. Tuli, R. N. Alief, D.-S. Kim, and J.-M. Lee, "Meta-learning: A digital learning management framework using blockchain for metaverses," *IEEE Access*, 2024.

[13] M. F. Rahaman, M. Golam, M. R. Subhan, E. A. Tuli, D.-S. Kim, and J.-M. Lee, "Meta-governance: Blockchain-driven metaverse platform for mitigating misbehavior using smart contract and ai," *IEEE Transactions on Network and Service Management*, 2024.

[14] S. Samarakoon, Y. Siriwardhana, P. Porambage, M. Liyanage, S.-Y. Chang, J. Kim, J. Kim, and M. Ylianttila, "5g-nidd: A comprehensive network intrusion detection dataset generated over 5g wireless network," *arXiv preprint arXiv:2212.01298*, 2022.

[15] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "Ciciot2023: A real-time dataset and benchmark for large-scale attacks in iot environment," *Sensors*, vol. 23, no. 13, p. 5941, 2023.