Blockchain-aided Collaborative Threat Detection for Securing Digital Twin-based IIoT Networks

Ahmad Zainudin[*†], Made Adi Paramartha Putra[§‡], Revin Naufal Alief[§], Dong-Seong Kim[§], and Jae-Min Lee[§]
[*]Department of Electronic Engineering, Kumoh National Institute of Technology, Gumi, South Korea
[§]Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, South Korea
[†]Department of Electrical Engineering, Politeknik Elektronika Negeri Surabaya, Surabaya, Indonesia
[‡]Faculty of Information Technology and Design, Primakara University, Denpasar, Indonesia
(zai*, mdparamartha95, revinnaufal, dskim, ljmpaul)@kumoh.ac.kr

***Abstract*—The distributed and heterogeneous connections in the digital twin (DT)-based industrial Internet of Things (IIoT) are vulnerable to cyber-attacks and malicious activities. This study proposes a permissioned blockchain-assisted collaborative and decentralized cyber threat detection for securing DT-based IIoT networks. A context-aware network intrusion detection system (C-NIDS) model was developed using factorized and grouped convolution structures to detect adversarial attacks in virtual and physical environments. A verifiable off-chain aggregation technique with a digital signature is implemented to provide a trustworthy and anti-tampering aggregated model with minimum transaction time. The results exhibit the robustness of the proposed model by achieving an attack detection accuracy of 99.50% using a lightweight model structure with trainable parameters of $4,634$ and MFLOPs calculation of 0.0088. Moreover, the verifiable off-chain aggregation performs a total transaction time of 0.0244 seconds.**

***Index Terms*—Collaborative intrusion detection, blockchain, verifiable off-chain aggregation, digital twin, industrial internet of things (IIoT)**

I. Introduction

The industrial Internet of Things (IIoT) is an advanced IoT application with numerous connections of industrial devices, control systems, and intelligent decisions to realize Industry 4.0. Distributed edge learning, digital twin (DT), next-generation wireless network, massive Internet of Things (IoT), and blockchain empower emerging intelligent IIoT to enhance efficiency, precision, and security in manufacturing production [1]. DT facilitates a digital representation of the physical environment by utilizing massive data and enabling control signals from the digital environment. The developing DT-based IIoT digitalizes dynamic and complex industrial environments to capture real-time processing and provide autonomous critical decision-making. Furthermore, DT becomes a catalyst for realizing future industrial cyber-physical systems (CPS) and is expected to be a critical advanced technology in future 6G wireless networks. Nevertheless, DT-empowered industrial CPS's heterogeneous and distributed connections are susceptible to several cyber threats and malicious network activities [2]. The massive interactions between industrial physical, virtual, and cyber domains extend adversarial vulnerabilities. Cybercriminals might exploit DTs to infiltrate and target the physical environment assets that are replicated. Moreover, increasingly advanced and sophisticated threats make the safety of DT-based IIoT challenging [3]. Therefore, ensuring security becomes a pressing concern in the context of DT-empowered IIoT.

Machine learning (ML) and deep learning (DL) based intrusion detection systems (IDS) were widely developed to identify and mitigate the cyber attacks in IIoT networks [4]. A data poisoning attacks-robust anomaly detection for DT-based networks was implemented in [5]. This system constructed the poisoning attacks and evaluated their effectiveness against the proposed ML-based anomaly detector. However, this approach used a centralized learning approach that posed several challenges, such as high communication overhead, data privacy, and leading to scalability issues. Using federated learning (FL), the distributed IDS offers collaborative training in edge devices with computing capabilities to address the limitations of centralized learning approaches [6]. In [7], an IDS framework was developed using federated meta-learning and DT with robust imbalanced data for a metaverse environment. This system conducted clustering within the FL environment for client grouping based on data distribution to address the statical heterogeneity and enhance global model performance. However, this method utilizes the centralized aggregation mechanism, vulnerable to a single point of failure (SPoF) and distributed denial-of-service (DDoS) attacks.

Blockchain is widely utilized for several applications to facilitate traceability, integrity, and trustworthy data management. Employing FL and blockchain to develop an IDS framework can provide a reliable model with trustworthiness for FL entities and traceability model exchange capabilities. The authors [8] deployed a distributed DT-based anomaly detection architecture using edge learning and blockchain. The system focuses on constructing a self-healing technique and decentralized trust management in IIoT. Several DL models were compared and evaluated using WADI, SwaT, and BATADAL datasets. In [9], the blockchain was utilized to ensure the trustworthiness of DT-empowered IIoT. This system implemented a blockchain and DL integration framework to provide secure authenticity and integrity of the data. The hybrid Long Short Term Memory-Sparse AutoEncoder (LSTM-SAE) and Bidirectional Gated Recurrent Unit (BiGRU) model

ICC 2024 - IEEE International Conference on Communications | 978-1-7281-9054-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICC51166.2024.10622717

TABLE I
COMPARISON BETWEEN PROPOSED SYSTEM AND EXISTING IDS FRAMEWORK FOR DT-BASED IIOT NETWORKS

Ref	Target System	Method	Dataset	DL	DA	Tw	Vr	DS	TB	LGC
[5]	DT-based Network	DT, RF, DNN	CICIDS-2017	✗	✗	✗	✗	✗	✗	✗
[7]	DT, Metaverse	FML-DT	UNSW-NB-15, NSL-KDD	✓	✗	✗	✗	✗	✗	✗
[8]	DT-based IIoT	LSTM, GAN, IF	WADI, SwaT, BATADAL	✓	✗	✓	✗	✗	✗	✗
[9]	DT-based IIoT	LSTMSAE, BiGRU	CICIDS-2017, ToN-IoT	✓	✓	✓	✗	✗	✗	✗
Ours	DT-based IIoT	BCFed-DT	N-BaIoT	✓	✓	✓	✓	✓	✓	✓

*__DL__: Decentralized Learning, *__DA__: Distributed Aggregation, *__Tw__: Trustworthiness, *__Vr__: Verifiability, *__DS__: Digital Signature, *__TB__: Time-aware Blockchain, *__LGC__: Low Gas Cost, ✓: Considered, ✗: Non-Considered

was developed using CICIDS-2017 and ToN-IoT datasets to identify cyber-attacks. However, these approaches [8], [9] have a high computation cost and leverage an on-chain mechanism for model storage every communication round in the integrated blockchain-FL environments. Implementing a full on-chain mechanism for FL with high-frequency transactions requires a high gas fee and processing time [10].

The existing conventional IDS approaches [5], [7]–[9] are inapplicable directly for cyber threat detection in the DT environments. The DT-based IIoT ecosystems generate vast amounts of data, and existing traditional IDS approaches may not efficiently be equipped to process and analyze this data for cyber threat detection. Moreover, cyber attackers may exploit vulnerabilities in the physical system and the DT environment, increasing the complexity of the attack surface. The summary of recent methods and the proposed system is compared in Table I. The proposed system provides several features, including decentralized learning (DL), distributed aggregation (DA), trustworthiness (Tw), verifiability (Vr), time-aware blockchain (TB), and low gas cost (LGC) mechanisms. Considering the essential of a privacy-preserving and trusted cyber attack detection framework with a low-complexity IDS model for DT-based IIoT networks, this study proposes potential contributions as follows:

1) We proposed a blockchain-assisted collaborative cyber threat detection with a verifiable off-chain aggregation mechanism for DT-based IIoT networks. An integration between permissioned blockchain and distributed interplanetary file system (IPFS) as the off-chain storage was utilized to provide trusted and anti-tampering model aggregation with minimum transaction time.
2) We introduced a verifiable off-chain aggregation technique by utilizing a (Rivest–Shamir–Adleman) RSA-based digital signature algorithm for securing and verifying content identifier (CID) data exchange between aggregator and FL clients.
3) We implemented a decentralized and collaborative context-aware cyber threat detection using the FL technique to enable privacy-preserving with high accuracy to detect malicious network activities in the physical and virtual environments of the DT-empowered IIoT networks.
4) We developed a lightweight IDS model using factorized and grouped convolution configurations to extract more depth features, enhance model effectiveness, and deliver a low-complexity model structure.

The rest of this paper is organized as follows: Section II explains the proposed blockchain-based collaborative cyber threat detection for DT-empowered IIoT networks. The extensive experiment results and discussion are presented in Section III-B. Finally, the conclusion of this study and some ideas for future works are described in Section IV.

II. BLOCKCHAIN-BASED COLLABORATIVE CYBER THREAT DETECTION FOR DT-BASED IIOT

A. Problem Formulation

The heterogeneous connections and massive interaction between physical and virtual environments in DT-based IIoT networks are vulnerable to cyber threats [2]. To mitigate this IIoT network vulnerability, several approaches were deployed [4], [5]. However, most of these methods used a centralized DL technique with several limitations, such as communication overhead, data privacy, and scalability issues. Some researchers applied an FL technique to develop a reliable IDS framework for industrial applications by avoiding sharing the raw data [6], [7]. However, the vanilla FL method requires a centralized aggregation coordinator to aggregate and calculate the global model. This scenario poses an SPoF and is vulnerable to malicious aggregators. Integrating the blockchain with the FL technique can provide trusted FL entities with an immutable model exchange and mitigate data poisoning. However, the existing integrated blockchain-FL approaches [10], [11] have high transaction time issues. DT ecosystem generates vast data, running complex and dynamic systems. Consequently, the current conventional IDS approaches cannot be used to identify cyber threats directly in the DT environment. A reliable and trusted cyber threat detection framework with high-precision capability for a dynamic and complex system in virtual and physical environments is still an open issue that needs to be solved. Therefore, this study integrates the FL and time-aware permission blockchain for developing a lightweight decentralized IDS framework with a verifiable off-chain aggregation mechanism for DT-based IIoT networks.

B. Proposed Systems

This study implements blockchain-aided collaborative cyber threat detection for securing DT-based IIoT networks. This system utilized a verifiable off-chain aggregation using IPFS

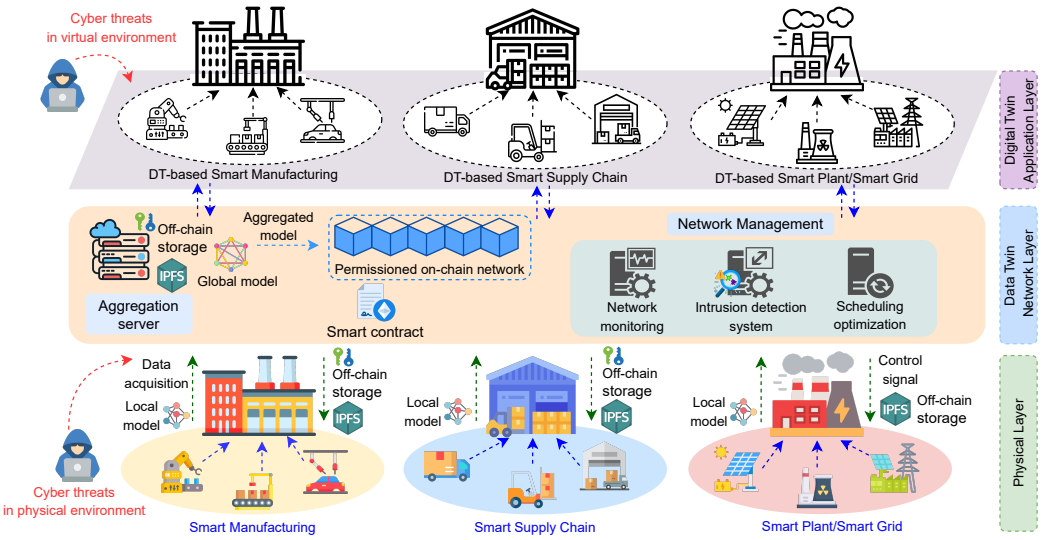

Fig. 1. Proposed blockchain-assisted collaborative cyber threats detection for DT-based IIoT networks

and RSA-based digital signature. A verifiable off-chain aggregation provides a trusted and anti-tampering decentralized model aggregation mechanism with low transaction time requirements. The proposed system is presented in Fig. 1 and consists of three layers: physical layer, data twin network layer, and DT application layers. The physical layer represents industrial edge servers E_n, where $n \in N = \{1, 2, 3, .., N\}$ denotes the FL clients with computation capabilities to conduct local training using captured local network data. In the data twin network layer, the aggregation server As aggregates the local model from all FL clients, calculates the global model, and stores it on the permissioned blockchain. The smart contract is developed to integrate blockchain and FL environments with several functions for storing and accessing the CID of local and global models. For network management purposes, this layer enables several services, including network monitoring, IDS, scheduling optimization, and synchronization services.

C. Context-aware Network Cyber Threat Detection Model

The proposed BCFed-DT model is constructed by factorized and grouped convolution structures to extract more depth features, improve model effectiveness, and enable a low-complexity IDS model. A residual connection addresses the gradient vanishing issue and provides model learning efficiency. Moreover, the convolution layer uses the composite convolution configuration by combining convolution, batch normalization, and ReLU in a cascade structure. This configuration provides smoother and faster model convergence. The proposed model consists of two main modules: MFC (Multi-Flow Factorized Convolution) and MFGC (Multi-Flow Factorized Group Convolution) modules. The input of the MFC module is reshaped into $\mathbf{I} \in \mathrm{N}^{1 \times 115 \times 1}$ dimension and fed to 3×3 regular composite convolution layer with eight filters. The output of this layer is fed into a multi-flow 1×3 and 3×1 regular composite convolution with factorized structure. A depth concatenate layer combines the output of the asymmetric composite convolution from the previous step to enhance the diversity of extracted features. The feature map F_{concat}^{MFC} from the depth concatenate operation of the MFC module is presented as follows:

$$\mathbf{F}_{concat}^{MFC} = \chi\left[\mathbf{F}_{3\times3}^{RC}\left(\mathbf{F}_{1\times3}^{RC}, \mathbf{F}_{3\times1}^{RC}\right)\right], \tag{1}$$

where, χ, $\mathbf{F}_{3\times3}^{RC}$, $\mathbf{F}_{1\times3}^{RC}$, and $\mathbf{F}_{3\times1}^{RC}$ represent the concatenate operation, regular composite convolution with kernel sizes 3×3, 1×3, and 3×1, respectively. Subsequently, a max-pooling $(2,2)$ layer is used to reduce spatial feature dimension. The reduced features are fed to 1×1 regular composite convolution with eight filters and ReLU activation, added with a residual connection block. This block comprises a $(2,2)$ max-pooling, 1×1 regular composite convolution, and ReLU layers. The additional operation of the MFC output $\mathbf{F}_{MFC}$ is presented as follows:

$$\mathbf{F}_{MFC} = \left(\mathbf{F}_{1\times1}^{RC}\left(\mathbf{F}_{concat}^{MFC}\right)\right) + \mathbf{F}_{1\times1}^{RC}\left(\mathbf{F}_{3\times3}^{RC}\right), \tag{2}$$

here, $\mathbf{F}_{1\times1}^{RC}$ denotes the regular composite convolution with eight filters and 1×1 kernel size.

Afterward, the output of the MFC module is fed to the MFGC module. This module facilitates feature extraction using 3×3 regular composite convolution layer with eight filters and multi-flow 16 filters 1×3 and 3×1 grouped composite convolution. The asymmetric features from the multi-flow structure in the previous step are combined using depth concatenate operation. The concatenated features of the MFGC module $\mathbf{F}_{concat}^{MFGC}$ are presented as follows:

$$\mathbf{F}_{concat}^{MFGC} = \chi\left[\mathbf{F}_{3\times3}^{RC}\left(\mathbf{F}_{1\times3}^{RGC}, \mathbf{F}_{3\times1}^{RGC}\right)\right], \tag{3}$$

where, χ, $\mathbf{F}_{3\times3}^{RC}$, $\mathbf{F}_{1\times3}^{RGC}$, $\mathbf{F}_{3\times1}^{RGC}$ represent the depth concatenate operation, 3×3 regular composite convolution with eight filters, 1×3 group composite convolution with 16 filters, and 3×1 group composite convolution with 16 filters, respectively.

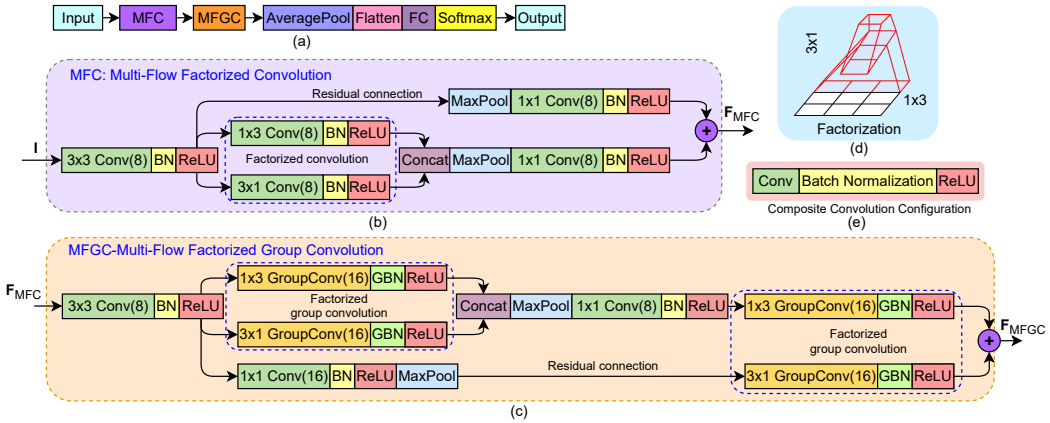

Fig. 2. Proposed context-aware BCFed-DT model for cyber threat detection in DT-based IIoT networks

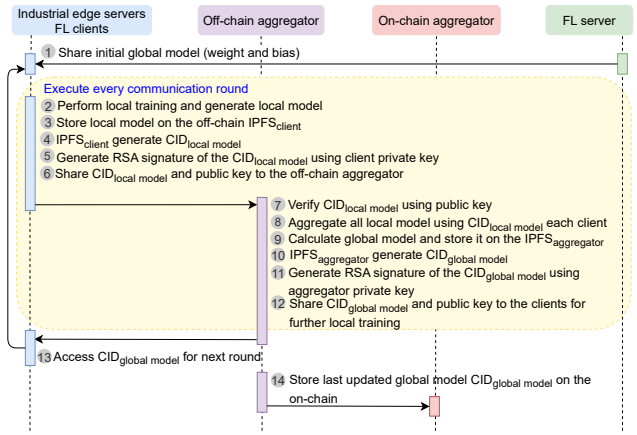

Fig. 3. Verifiable off-chain aggregation mechanism in collaborative cyber threat detection system

In sequence, the dimension of concatenated feature $\mathbf{F}_{concat}^{MFGC}$ is reduced using $(2,2)$ max-pooling layer and fed to the 1×1 regular composite convolution. In the final step of the MFGC module, an additional operation is used to add the output of the last multi-flow 1×3 and 3×1 group composite convolution layers. The output of MFGC module $\mathbf{F}_{MFGC}$ is presented as follows:

$$\mathbf{F}_{MFGC} = \mathbf{F}_{1\times3}^{RGC}\left(\mathbf{F}_{1\times1}^{RC}\left(\mathbf{F}_{concat}^{MFGC}\right)\right) + \mathbf{F}_{3\times1}^{RGC}\left(\mathbf{F}_{1\times1}^{RC}\right). \quad (4)$$

where, $\mathbf{F}_{1\times3}^{RGC}\left(\mathbf{F}_{1\times1}^{RC}\left(\mathbf{F}_{concat}^{MFGC}\right)\right)$ represents a group composite convolution process the 1×1 regular composite convolution result with concatenated feature as the input, and $\mathbf{F}_{3\times1}^{RGC}\left(\mathbf{F}_{1\times1}^{RC}\right)$ denotes the 3×1 group composite convolution with a residual connection result as the input. Subsequently, the extracted feature of MFGC module $\mathbf{F}_{MFGC}$ is processed to $(2,2)$ average-pooling layer to decrease spatial dimension and enable low computational complexity in a fully connected layer. Finally, a softmax activation is utilized to classify the probability of cyber threats in IIoT networks.

D. Verifiable Off-Chain Aggregation Technique

To reduce blockchain transaction time issues in the existing integrated blockchain-FL approaches [10], [11], this study applied a verifiable off-chain aggregation mechanism using RSA-based digital signature as is presented in Fig. 3. At the first round r, where $r \in R = \{1,2,3,..,R\}$, the FL server shares the initial global model with all available industrial edge server FL clients to perform local training using captured network local data and generate the local model, denoted as the $m_{n,r}^{local}$. The FL clients store $m_{n,r}^{local}$ on the off-chain IPFS_n^{local} and generate an CID $\text{CID}_{n,r}^{local}$. The CID is a string of characters that provides a unique identifier of a resource available on the IPFS. The clients generate 1024-bit RSA key-pair and sign the $\text{CID}_{n,r}^{local}$ using the RSA private key $\{n,d\}$, where n and d are typically big integers. Subsequently, calculate their hash h using SHA-512 and encrypt h to execute the signature $sign_{local}^{\text{CID}}$, as follows:

$$h = \text{hash}(\text{CID}_{n,r}^{local}), \quad (5)$$

$$sign_{local}^{\text{CID}} = h^d \,(\text{mod}\, n). \quad (6)$$

The FL clients share the signed $\text{CID}_{n,r}^{local,signed}$ and original $\text{CID}_{n,r}^{local}$ to the off-chain aggregator. The off-chain aggregator verifies the $\text{CID}_{n,r}^{local,signed}$ using the public key of each client. If verified, the off-chain aggregator collects all local models by accessing $\text{CID}_{n,r}^{local}$ and calculates the global model using a particular aggregation algorithm. The updated global model m_r^{global} is stored on the off-chain and generates the global model CID_r^{global}. Like the local model, sharing CID_r^{global} to the clients for further local training employed an RSA-based digital signature to ensure without tampering by attackers. At the last round, the updated global model CID_R^{global} is stored on the permissioned on-chain network. Implementing a verifiable off-chain aggregation technique, the aggregation process is not required to communicate with the on-chain network to generate a new block for storing an updated global model every round. Therefore, this approach can significantly reduce the blockchain transaction time in the blockchain-FL system.

III. Experimental Results and Discussion

This section evaluates the proposed collaborative cyber threat detection and verifiable off-chain aggregation technique.

TABLE II
CLASSIFICATION PERFORMANCE OF BCFED-DT MODEL WITH DIFFERENT MODULE CONFIGURATION

Module Configuration	Accuracy	Precision	Recall	F1-Score	Loss	Trainable Parameters	Model Size	MFLOPs
Without MFC	96.52%	96.25%	96.05%	96.06%	0.0849	5,602	21.88 KB	0.0108
Without MFGC	97.82%	97.67%	97.52%	97.54%	0.0803	**3,098**	**12.10 KB**	**0.0061**
One MFC and One MFGC	**99.50%**	**99.44%**	**99.45%**	**99.44%**	**0.0168**	4,634	18.10 KB	0.0088
Two MFC and Two MFGC	99.32%	99.25%	99.26%	99.25%	0.0186	6,178	24.13 KB	0.0115
Two MFC and Three MFGC	99.27%	99.19%	99.20%	99.19%	0.0226	7,890	30.82 KB	0.0145
Three MFC and Two MFGC	99.37%	99.33%	99.30%	99.31%	0.0218	7,438	28.65 KB	0.0127

TABLE III
COMPARISON OF EXISTING COLLABORATIVE THREAT DETECTION TECHNIQUES FOR DT AND BLOCKCHAIN-BASED IIOT NETWORKS

Method	Accuracy	Precision	Recall	F1-Score	Loss	AUC Score	Trainable Parameters	Model Size	MFLOPs
DNN [5]	99.06%	99.01%	98.92%	98.95%	0.0411	0.9939	25,514	99.66 KB	0.0505
IDSFedNet [6]	99.31%	99.23%	99.24%	99.23%	0.0225	0.9960	13,928	54.41 KB	0.0267
FML-DT [7]	99.34%	99.27%	99.28%	99.27%	0.0213	0.9960	2,458,506	9.38 MB	4.9141
MiTFed [11]	99.02%	98.91%	98.93%	98.91%	0.0333	0.9938	45,394	177.32 KB	0.0901
Proposed BCFed-DT	**99.50%**	**99.44%**	**99.45%**	**99.44%**	**0.0168**	**0.9962**	**4,634**	**18.10 KB**	**0.0088**

This system utilizes a Flower 1.1.0 framework to develop an FL environment and Hyperledger Besu to create a permissioned blockchain network. The IIoT-related benchmarks N-BaIoT dataset [12] is used to validate the proposed model.

A. Collaborative Cyber Threats Detection Performance

Table II presents the classification performance of the proposed BCFed-DT model with different module configurations. This analysis aims to validate the module architecture with high accuracy and a low-complexity model structure. Based on the results, the model configuration with one MFC and one MFGC module structure has the highest performance and achieves an accuracy of 99.50%, a precision of 99.44%, a recall of 99.45%, an F1-score of 99.44%, and a loss of 0.0168. In addition, this architecture has $4,634$ trainable parameters, 18.10 KB model size, and 0.088 MFLOPs calculation. Another model configuration, without an MFGC module structure, has lower trainable parameters, model size, and MFLOPs calculation. However, that module configuration has low accuracy, precision, recall, and F1-score performances.

The comparison analysis between the proposed model and existing methods of collaborative threat detection for DT and blockchain-based IIoT networks is presented in Table III. This analysis compares various methods, such as DNN [5], IDSFedNet [6], FML-DT [7], and MiTFed [11]. The comparison was conducted by re-running the existing methods with the same environment and learning parameters. The DNN [5] utilized three layers of Dense and performed an accuracy of 99.06% with $25,514$ trainable parameters and 0.0505 MFLOPs calculation. The IDSFedNet [6] used a CNN-MLP model with grouped and factorized configurations. This model achieved 99.31% of accuracy with trainable parameters of $13,928$. The FML-DT [7] employed a ResNet-9 model and achieved 99.34% of accuracy with $2,458,506$ trainable parameters. The MiTFed [11] model was conducted by three Dense layers with 122 neurons. This model achieved an accuracy of 99.02% and a MFLOPs calculation of 0.0901. Based on this comparison, the accuracy performance of the proposed BCFed-DT is closer to that of the existing methods. However, BCFed-DT achieved a higher accuracy of 99.50% with a low model complexity structure.

B. Blockchain-based Aggregation Performance

Fig. 4 presents the transaction time of the off-chain aggregation mechanism, including store global model, access global model, store local model, and access local model transactions. This evaluation measures the transaction time of storing the global and local models on the IPFS and generates the CID. Furthermore, the transaction time of model accessing from IPFS was measured to ensure the reliability of the proposed technique. Based on the results, the off-chain aggregation performed 9.601 ms for the average store global model time, 2.425 ms for the average access global model time, 9.236 ms for the average store local model time, and 2.277 ms for the average access local model time. The transaction time of on-chain aggregation with various consensus algorithms (QBFT, IBFT 2.0, and Ethash) is presented in Fig. 5 and Fig. 6. This measurement shows that QBFT consensus outperforms other consensuses with performed 1.984 seconds for storing aggregated global models on the permission blockchain network. On the other hand, the IBFT 2.0 achieved the lowest transaction time of 0.008 seconds for accessing the aggregated global model from the on-chain network. The QBFT and IBFT 2.0 consensuses perform similarly due to a proof-of-authority (PoA)-based consensus algorithm. The digital signature integration with blockchain-based aggregation mechanism performance is presented in Fig. 7. The computation time of data signing using RSA requires 0.691 ms and 0.208 ms for data verifying. Based on these results, implementing a digital signature in an off-chain aggregation mechanism is suitable for providing a verifiable, low-latency, and trusted model exchange and aggregation.

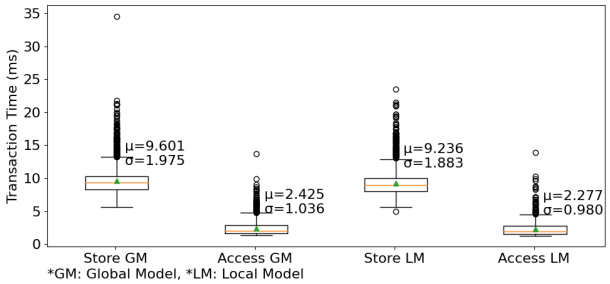

Fig. 4. Transaction time of off-chain aggregation (store GM, access GM, store LM, and access LM)

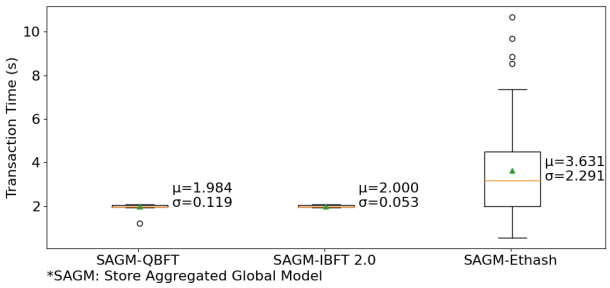

Fig. 5. Transaction time of storing aggregated global model for on-chain aggregation with different consensus algorithms

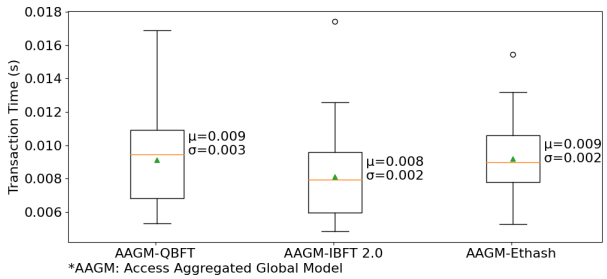

Fig. 6. Transaction time of accessing aggregated global model for on-chain aggregation with different consensus algorithms

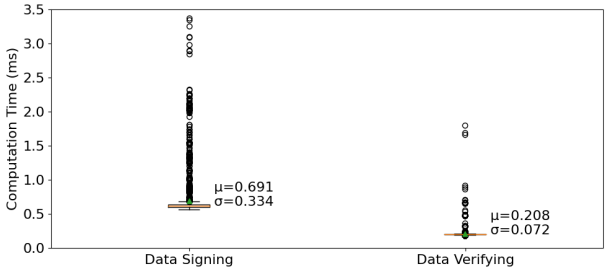

Fig. 7. Computation time of RSA-based digital signature for anti-tampering off-chain aggregation

IV. Conclusion

This paper integrates blockchain and FL techniques to develop collaborative cyber threat detection with a verifiable off-chain aggregation mechanism for securing DT-based IIoT networks. The proposed verifiable off-chain aggregation utilized trusted decentralized IPFS storage and RSA-based digital signature to provide trustworthy model aggregation with minimum transaction time. Based on the measurement results, the proposed context-based BCFed-DT model outperforms existing threat detection techniques by achieving a high accuracy detection and has a low complexity model structure. For future work, consider delay-aware integrated private and public blockchains with a more secure model exchange mechanism for collaborating threat detection in a DT-based smart factory environment.

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the Institute of IITP grant funded by the Korea government(MSIT) (IITP-2024-2020-0-01612, 50%) and by Priority Research Centers Program through the NRF funded by the MEST(2018R1A6A1A03024003, 50%).

References

[1] W. Yang, W. Xiang, Y. Yang, and P. Cheng, "Optimizing Federated Learning with Deep Reinforcement Learning for Digital Twin Empowered Industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1884–1893, 2022.

[2] A. De Benedictis, F. Flammini, N. Mazzocca, A. Somma, and F. Vitale, "Digital Twins for Anomaly Detection in the Industrial Internet of Things: Conceptual Architecture and Proof-of-Concept," *IEEE Transactions on Industrial Informatics*, 2023.

[3] 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.

[4] 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*, 2022.

[5] S. Li, W. Wu, Y. Meng, J. Li, H. Zhu, and X. S. Shen, "Data Poisoning Attack against Anomaly Detectors in Digital Twin-Based Networks," in *2023 IEEE International Conference on Communications (ICC): Communication and Information System Security Symposium*. IEEE, 2023, pp. 13–18.

[6] A. Zainudin, R. Akter, D.-S. Kim, and J.-M. Lee, "Federated Learning Inspired Low-Complexity Intrusion Detection and Classification Technique for SDN-Based Industrial CPS," *IEEE Transactions on Network and Service Management*, 2023.

[7] S. He, C. Du, and M. S. Hossain, "6G-enabled Consumer Electronics Device Intrusion Detection with Federated Meta-Learning and Digital Twins in a Meta-Verse Environment," *IEEE Transactions on Consumer Electronics*, 2023.

[8] X. Feng, J. Wu, Y. Wu, J. Li, and W. Yang, "Blockchain and Digital Twin Empowered Trustworthy Self-Healing for Edge-AI enabled Industrial Internet of Things," *Information Sciences*, vol. 642, p. 119169, 2023.

[9] 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*, 2022.

[10] A. Zainudin, R. N. Alief, M. A. P. Putra, D.-S. Kim, and J.-M. Lee, "Blockchain-Based Decentralized Trust Aggregation for Federated Cyber-Attacks Classification in SDN-Enabled Maritime Transportation Systems," in *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2023, pp. 182–187.

[11] Z. Abou El Houda, A. S. Hafid, and L. Khoukhi, "MiTFed: A Privacy Preserving Collaborative Network Attack Mitigation Framework Based on Federated Learning using SDN and Blockchain," *IEEE Transactions on Network Science and Engineering*, 2023.

[12] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-BaIoT—Network-based Detection of IoT Botnet Attacks using Deep Autoencoders," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, 2018.