Enhancing IIoT Security Using Hybrid CNN-BiLSTM Models with Blockchain Integration

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

***Abstract*—In the rapidly evolving Industrial Internet of Things (IIoT) landscape, ensuring robust security measures for detecting and mitigating cyber threats is paramount. This paper suggests a decentralized intrusion detection system (IDS) that uses Federated Learning (FL) integrated with a permissioned blockchain layer to secure IIoT networks. The system leverages a modified deep learning architecture, staking Convolutional Neural Networks (CNN) with Bidirectional Long Short-Term Memory (BiLSTM) and Long Short-Term Memory (LSTM) layers to quickly detect the temporal and spatial sequences in data traffic over a network. Training the model in a federated environment ensures data privacy, and the blockchain layer guarantees that only authorized devices participate in the learning process, adding an extra layer of security. We evaluated our model using the Edge-IIoTset dataset, containing 14 cyber-attack types and one benign class. Our suggested model showed superior performance, achieving an accuracy of 95%, surpassing traditional models' accuracy in similar environments.**

***Index Terms*—Federated Learning, Neural Network, BiLSTM, CNN, Edge Iot**

I. Introduction

Industrial Internet of Things (IIoT) involves interconnected sensors, devices [1], and machines in industrial settings like manufacturing plants, energy grids, and smart factories. IIoT systems comprise large-scale distributed networks where numerous machines and devices generate vast data requiring rapid processing for operational efficiency [2]. These devices [3] produce highly heterogeneous data due to the diversity of sensors used in industrial processes [4], making it critical to defend against potential attacks [5], [6]. The data heterogeneity and myriads of devices pose significant challenges in attack detection [7], necessitating a robust mitigation architecture, which this study addresses with a permissioned private blockchain network integrated with an intrusion detection system (IDS).

Blockchain provides a decentralized, tamper-proof framework that enhances security and trust in federated learning-based IDS [8], [9]. By integrating blockchain with federated learning (FL), updates are securely shared among preregistered IIoT devices on a proof-of-authority blockchain network [8], [10], [11]. This network, spanning three tiers: industrial IoT devices, edge servers, and cloud servers, ensures trust and accountability [12]. The synergy between blockchain and FL enables decentralized intrusion detection, protecting data privacy and model integrity while allowing collaborative training [13]. This architecture provides industrial environments with secure, efficient threat detection and response [1], [14].

While blockchain secures data exchange across the network tiers [15], the IDS's performance heavily relies on processing and analyzing the diverse data from IIoT devices [16], [17]. The complexity and heterogeneity of IIoT environments require a robust neural network to detect known and emerging threats in real-time. Traditional machine learning models often fail to capture the intricate temporal and spatial patterns in IIoT network traffic. This paper proposes a hybrid model comprising Convolutional Neural Networks-Bidirectional Long Short Term Memory and Long Short Term Memory (CNN-BiLSTM-LSTM) for intrusion detection in IIoT environments.

The combination of CNN [18], [19] and BiLSTM [12], [20] networks allows the model to effectively capture spatial features from network traffic data and the temporal dependencies crucial for identifying sophisticated attack patterns. The addition of LSTM layers [12] further enhances the model's ability to process long-term dependencies, making it ideal for scenarios where real-time threat detection is critical. Integration of this hybrid neural network with the FL and blockchain creates an advanced, decentralized IDS that is secure and effective in detecting a wide range of cyber-attacks across industrial networks [20], [21]. Relative to the recent research, this paper contributes the following:

1) Designs and implements a combined CNN and BiLSTM framework for detecting intrusions in Internet of Things (IoT) network systems
2) Introduces an enhanced and definitive architectural design for IIoT that incorporates a blockchain layer to boost security.
3) Creates a protected Federated Learning pipeline with blockchain for training and distributing models within IIoT settings to verified nodes.

This paper is arranged thus: introduction in Section I is followed by Section II, the background study, and a review of existing works. Section III discusses the proposed framework and analysis of the experimental setup and performance. The result discussion is presented in Section IV. The study concludes in Section V, highlighting the contributions and potential future work.

II. Background of Study and Related Works

In the rapidly evolving IIoT networks, securing the vast and heterogeneous data generated by interconnected devices is a critical challenge [1]. As industries increasingly adopt edge computing to process data closer to its source [4], the risk of cyber-attacks and data breaches grows [6]. Traditional centralized intrusion detection systems struggle with the complexity and scale of IIoT environments, necessitating decentralized solutions [6].

Incorporating blockchain technology [5] into IIoT networks adds security by managing participant registration and ensuring only authorized devices interact within the network [14]. The permissioned blockchain excludes unauthorized participants, while a proof of authority (PoA) consensus mechanism secures the federated learning process. As noted by [8], [22], this approach ensures that only trusted devices participate in model updates, mitigating risks from poisoning attacks or compromised data. Integrating blockchain strengthens the security and reliability of the federated learning model, enhancing its resilience to adversarial activities.

A key challenge highlighted by [23] is that traditional intrusion detection approaches, while effective, struggle with the dynamic nature of IIoT environments [16]. Models such as feed-forward neural networks have shown promising results on datasets like BoT-IoT, [24] achieving high accuracy in detecting known attack patterns. However, they face limitations with increasingly complex datasets or high traffic volumes. To address these limitations, researchers have turned to deep learning techniques, particularly recurrent neural networks, such as LSTM, offering enhanced capabilities in handling large, diverse datasets [25], [26].

Centralized models, though accurate, suffer from latency and bandwidth limitations in IIoT environments [1], affecting real-time performance. Federated learning (FL) offers a solution by processing the local data at the edge and only sharing model updates, reducing data transmission and preserving privacy [15], [27]. Bi-LSTM models [26], effective in capturing temporal patterns and preventing overfitting, are well-suited for IIoT environments where data varies significantly [21], [24]. Hybrid architectures like CNN-BiLSTM-LSTM provide scalability for detecting cyber-attacks by efficiently processing high-dimensional data [28]. A tiered edge computing architecture further enhances scalability and real-time responsiveness, reducing latency and bandwidth usage while improving intrusion detection [28]. Combining FL with blockchain ensures a robust, scalable, and secure framework for IIoT networks.

III. Proposed System methodology

A. Blockchain Layer

The blockchain layer in our proposed system acts as a crucial security component, reinforcing the entire three-tier architecture by ensuring that only authorized devices are allowed to participate in the federated learning process. It functions as a permissioned blockchain network [12], meaning that all participating devices have their addresses securely registered on the blockchain. This creates a transparent and secure ecosystem where each device is aware of the other legitimate participants, effectively preventing unauthorized devices from accessing the network. The system employs a PoA consensus mechanism, which is responsible for verifying and authenticating the devices on the network.

Algorithm 1 Device Registration and Breach Notification

```
Require: address: device, list: devices, list: breaches
procedure REGISTERDEVICE(device)
    authorizedDevices[device] ← true
    NOTIFYALLCLIENTS(devices)
    emit DeviceRegistered(device)
end procedure
procedure UNREGISTERDEVICE(device)
    authorizedDevices[device] ← false
    NOTIFYALLCLIENTS(devices)
    emit DeviceUnregistered(device)
end procedure
procedure NOTIFYALLCLIENTS(devices)
    validDevices ← GETALLAUTHORIZEDDEVICES
    emit NotifyClients(validDevices)
end procedure
procedure GETALLAUTHORIZEDDEVICES
    authorized ← new list
    for device in devices do
        if authorizedDevices[device] = true then
            append device to authorized
        end if
    end for
    return authorized
end procedure
procedure NOTIFYBREACH(device)
    emit BreachNotification(device, "Security Breach Detected")
end procedure
procedure NOTIFYSERVERS(device)
    NOTIFYBREACH(device)
    emit NotifyServers(device, "Security Breach Alert")
end procedure
```

The code presented in the 1 outlines our smart contract's core functions and variables for managing device registration and handling breach notifications. The **RegisterDevice** function allows the admin to register a new device by setting its authorization status to true and emitting an event to notify all connected clients. On the other hand, **UnregisterDevice** removes a device by changing its status to false and emitting a similar event. The **NotifyAllClients** function ensures that all IIoT devices are kept informed of the updated list of authorized devices, maintaining network transparency. The **GetAllAuthorizedDevices** function iterates through the list of devices, verifies their authorization status, and returns a list of the approved devices. In the event of unauthorized access, **NotifyBreach** triggers an alert regarding the breach, while

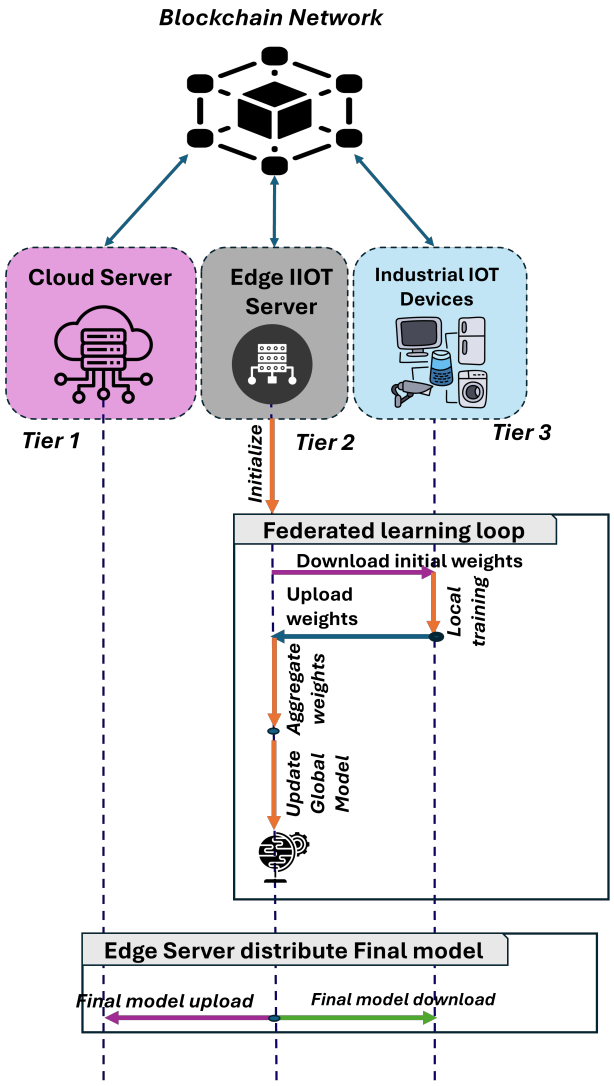

Fig. 1: The process flow of proposed architecture.

NotifyServers notifies both the cloud server and IIoT server to take immediate action. This structure ensures effective device management and real-time responses to breaches, safeguarding the system's integrity.

B. Three-Tier Architecture

As illustrated in Figure 1, the system setup outlines a robust three-tier architecture to support the training and deployment of an IDS in an IIoT environment. The tiers are designed to handle various computational tasks. At the same time, blockchain technology provides a security layer on top of the three tiers, ensuring that all participating devices are authenticated and authorized. The blockchain is permissioned, meaning only registered devices with verified addresses can join the network. Every device's address is stored on the blockchain, and all participants in the network can view the other devices, ensuring transparency and security within the system. The tiers are as follows:

1) Tier 1: This tier comprises IIoT devices that gather data and perform local training during federated learning. Devices receive initial model weights from the server, train locally, and upload updated weights. The Blockchain registration ensures device authenticity within the network.
2) Tier 2: In Tier 2, the IIoT server intermediates between the cloud server and IIoT devices, aggregating weights from Tier 1, updating the global model, and distributing initial weights for local training. It also manages federated learning iterations, while the blockchain secures the process by allowing only registered devices to upload weights for aggregation.
3) Tier 3: The cloud server, positioned in Tier 3, manages more complex operations. While Tier 1 and Tier 2 handle the iterative training, Tier 3 is designed to support other computational tasks on the network that require additional resources.

C. Federated Learning Setup

The architecture employs federated learning [15] between Tier 1 (IIoT devices) and Tier 2 (IIoT server), as shown in Figure 1. Tier 1 devices perform local training, while the Tier 2 server coordinates by aggregating uploaded weights and updating the global model. Using the Flower framework for scalability, the IIoT server distributes global weights, collects updated device weights, and applies the FedAvg algorithm for aggregation. This iterative process continues until the model achieves satisfactory accuracy.

D. Model Design

The model used in this system combines CNNs, BiLSTM, and LSTM units to optimize the detection and classification of network intrusions in IIoT environments [25]. The model's architecture begins with two Conv1D layers to capture spatial patterns from the data, followed by Max Pooling to reduce the computational complexity. Dropout layers are added to mitigate over-fitting during training.

The key components, BiLSTM and LSTM layers, process the data forward and backward, enabling the model to capture long-term dependencies in network traffic [20], [21]. This setup enhances the detection of subtle and complex attack patterns, making the model highly effective for multi-class intrusion detection. The BiLSTM layer structure is as in Equation 1

$$h_t^{\text{bi}} = \text{LSTM}_{\text{fwd}}(x_t, h_{t-1}^{\text{fwd}}) + \text{LSTM}_{\text{bwd}}(x_t, h_{t+1}^{\text{bwd}}), \quad (1)$$

Where h_t^{bi} is the BiLSTM hidden state at time step t, LSTM_{fwd} and LSTM_{bwd} represent the forward and backward LSTM states, respectively.

Succeeding is a Dense layer with 64 units, and ReLU activation is applied to refine the learned features further. Another dropout layer having 30% rate is added to further mitigate over-fitting. Finally, an output layer with 15 units and a Softmax activation function classify the input into one of 15 classes. The Sparse Categorical Cross entropy loss

function is used as it favors multi-class classification and is optimized using the Adam optimizer, known for its ability to automatically adjust learning rates during training.

E. Description of Dataset

The Edge-IIoTset dataset [1], used in our study, is specifically designed to capture the complexity of IoT and Industrial IoT (IIoT) environments. It contains a diverse collection of real-world network traffic, featuring 14 attacks and one benign class. These attacks range from Man-in-the-Middle (MitM) and Denial of Service (DoS) to Spoofing and Port Scanning, common threats in IIoT networks. By utilizing this dataset, we aimed to develop a distributed learning-based IDS capable of identifying cyber threats while distinguishing them from normal network traffic. The diversity of attack types and the inclusion of benign data ensured that our system was trained on a broad spectrum of scenarios, making it robust and adaptable to the real-time challenges of IIoT networks.

IV. Performance Evaluation and Result Discussion

The graph in Figure 2 shows the learning pattern of our hybrid model. While the training process takes some time due to the complexity of the model and the federated learning framework, it is notable that our model achieves high accuracy within a minimal number of rounds. By **Round 5**, the model reaches an impressive accuracy of 90%, and by **Round 10**, the accuracy plateaus at 95%, showing that the model converges quickly. At the same time, the loss decreases sharply, starting at 4.0 in the first round and dropping to 0.061 by the final round. These metrics demonstrate that the model learns rapidly, achieving high accuracy while maintaining a relatively low number of training rounds.

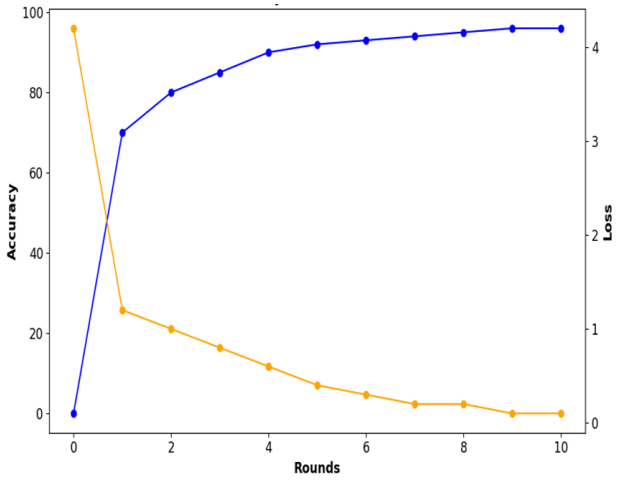

Fig. 2: Graph showing the learning path of the aggregation

Figure 3 shows the learning path for a centralized CNN-BiLSTM proposed by the authors in [26]. Our proposed FL model demonstrates a smoother learning curve than the centralized model. However, the centralized model benefits from faster convergence due to direct access to the dataset but sacrifices stability and raises privacy concerns, which our private blockchain addresses in our proposed FL architecture.

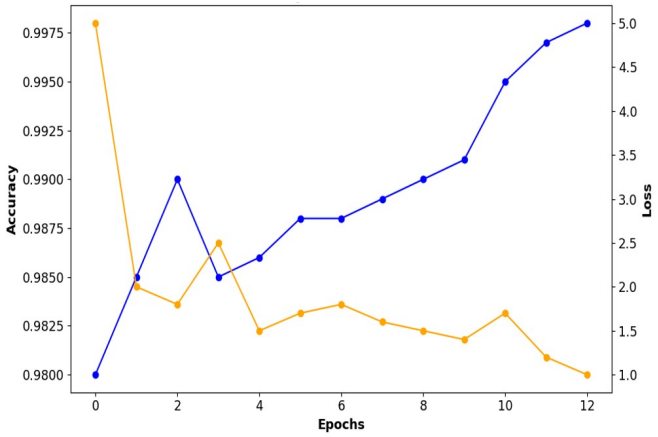

Fig. 3: Learning path of Centralised CNN-BiLSTM model [26] on UNSW NB15 open dataset

Furthermore, the confusion matrix 4 demonstrates that our intrusion detection model performs exceptionally well across various attack classes, achieving high accuracy for most. For instance, Class 0 reaches an accuracy of 91.27%, while attack types such as Class 2 and Class 3 achieve 100% classification accuracy, highlighting the model's robustness in detecting specific intrusions. However, certain classes, like Class 5, show lower accuracy at 60.44%, suggesting challenges in distinguishing these types of attacks, particularly in complex traffic scenarios. Despite these discrepancies, the model maintains strong performance across most classes, reinforcing its real-time IIoT intrusion detection effectiveness. The Receiver

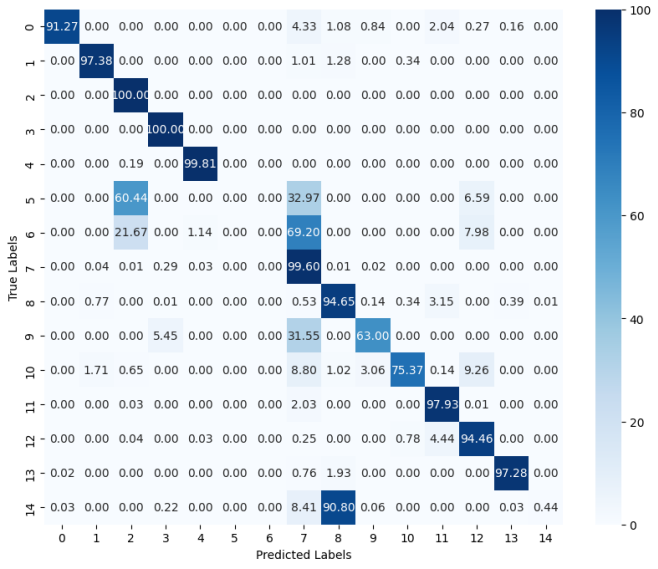

Fig. 4: Confusion matrix visualizing the model performance.

Operating Characteristic (ROC) curve in Figure 5 exhibits exceptional performance across all classes of our model, with

TABLE I: Comparison of Related Work

Study	Models Used	Dataset	Target System	Learning Type	Blockchain	Overall Accuracy (%)
[24]	DeepAK-IoT model	TON-IoT,Edge-IIoT, UNSW-NB15	IoT	CL	No	94.96
[5]	Contractive Sparse Autoencoder (CSAE), ABiLSTM	TON-IoT, Edge-IIoT	IIoT	CL	Yes	93
[1]	DecisionTree, RFF, KNN, Deep Neural Network	Edge-IIoT	IIoT	CL/FL	No	93.22 (FL)
This work	**Hybrid-CNN-BLSTM-LSTM**	**Edge-IIoT**	**IIoT**	**FL**	**Yes**	**95**

area under the curve values ranging from 0.98 to 1.00. The curves approximate the top-left corner, indicating superior classification capabilities. The model effectively differentiates between classes while maintaining high predictive accuracy, thus validating the robustness of its training and aggregation process, as the confusion matrix shows.

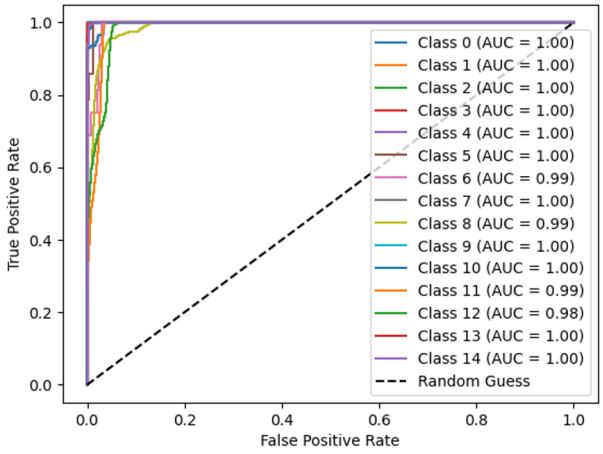

Fig. 5: ROC illustrating the model performance.

A. Result Discussion

The Hybrid-CNN-BLSTM-LSTM model we proposed demonstrates superior performance due to its unique ability to detect spatial and temporal features in IIoT network traffic data, which is essential for detecting complex cyber-attacks. The CNN layers excel at extracting spatial patterns from high-dimensional network data, making the model adept at identifying the unique signatures of different attack types. The addition of Bidirectional LSTM [20], [21] layers enhances the model's capability to learn from both past and future time steps, which is particularly valuable in detecting multi-stage or slow-propagating attacks that develop over time.

The LSTM component further processes long-term dependencies, enabling the model to retain critical information from earlier sequences in the network traffic, which is vital for accurately detecting subtle or prolonged attacks. Combining these architectures allows the model to differentiate between various types of attacks. It contributes to its high performance across different attack classes, as evidenced by the confusion matrix.

Table I compares our proposed work to previous research; several distinctive features set our system apart, particularly the integration of federated learning and a blockchain layer for enhanced security and efficiency in IIoT environments. Unlike prior works, such as study [24], which employs a centralized learning architecture, our model uses a decentralized Federated Learning approach, eliminating the need for raw data transmission to a central server and ensuring data privacy at the edge. The Hybrid-CNN-BLSTM-LSTM model provides a robust solution for intrusion detection by combining both spatial and temporal learning, resulting in a 95% accuracy using the Edge-IIoTset dataset, which is superior to the 93% accuracy achieved by other models like the contractive sparse autoencoder and BiLSTM in study [5].

Moreover, the key differentiating factor is the blockchain layer integrated into our three-tier architecture. The blockchain ensures that only authorized devices can participate in the learning process, operating on a permissioned blockchain network where all participating devices are registered and authenticated via a PoA consensus mechanism. This mechanism secures the learning process and provides transparency, as all legitimate devices know each other. For instance, although study [5] employs blockchain, it does not implement the full spectrum of security our smart contract offers, such as breach notifications and real-time alerts to IIoT and cloud servers. By combining these advanced features with the scalability of FL, our system offers a more secure, efficient, and scalable solution for real-time intrusion detection in IIoT environments, surpassing the performance and security capabilities of prior works.

V. Conclusion

This research presents a novel approach to securing IIoT environments by integrating Federated Learning with a permissioned blockchain and a hybrid CNN-BiLSTM-LSTM model. Our proposed system addresses the challenges of intrusion detection in complex and large-scale industrial networks by ensuring data privacy and system security through decentralized learning and blockchain authentication. The hybrid neural network enhances the model's ability to detect a wide range of cyber threats by capturing spatial and temporal traffic patterns. With a demonstrated accuracy of 95% on the Edge-IIoTset dataset, this approach outperforms centralized models while providing additional layers of security and transparency. Our contributions offer significant advancements in IIoT security, and future work will focus on optimizing computational efficiency and further refining the model's ability to detect more sophisticated attack patterns.

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-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] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning," *IEEE Access*, vol. 10, pp. 40 281–40 306, 2022.

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

[3] S. Hamdan, M. Ayyash, and S. Almajali, "Edge-Computing Architectures for Internet of Things Applications: A Survey," *Sensors*, vol. 20, no. 22, p. 6441, 2020.

[4] A. Yazdinejad, B. Zolfaghari, A. Dehghantanha, H. Karimipour, G. Srivastava, and R. M. Parizi, "Accurate Threat Hunting in Industrial Internet of Things Edge Devices," *Digital Communications and Networks*, vol. 9, no. 5, pp. 1123–1130, 2023.

[5] A. Aljuhani, P. Kumar, R. Alanazi, T. Albalawi, O. Taouali, A. N. Islam, N. Kumar, and M. Alazab, "A Deep Learning Integrated Blockchain Framework for Securing Industrial IoT," *IEEE Internet of Things Journal*, 2023.

[6] M. Mohy-Eddine, A. Guezzaz, S. Benkirane, and M. Azrour, "An Effective Intrusion Detection Approach Based on Ensemble Learning for IIoT Edge Computing," *Journal of Computer Virology and Hacking Techniques*, vol. 19, no. 4, pp. 469–481, 2023.

[7] 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.

[8] A. Qammar, A. Karim, H. Ning, and J. Ding, "Securing Federated Learning with Blockchain: A Systematic Literature Review," *Artificial Intelligence Review*, vol. 56, no. 5, pp. 3951–3985, 2023.

[9] S. Ali, Q. Li, and A. Yousafzai, "Blockchain and Federated Learning-Based Intrusion Detection Approaches for Edge-Enabled Industrial IoT Networks: A Survey," *Ad Hoc Networks*, vol. 152, p. 103320, 2024.

[10] S. Ismail, S. Dandan, D. W. Dawoud, and H. Reza, "A Comparative Study of Lightweight Machine Learning Techniques for Cyber-Attacks Detection in Blockchain-Enabled Industrial Supply Chain," *IEEE Access*, 2024.

[11] A. Nazir, J. He, N. Zhu, M. S. Anwar, and M. S. Pathan, "Enhancing IoT Security: A Collaborative Framework Integrating Federated Learning, Dense Neural Networks, and Blockchain," *Cluster Computing*, pp. 1–26, 2024.

[12] S. Siami-Namini, N. Tavakoli, and A. S. Namin, "The Performance of LSTM and BiLSTM in Forecasting Time Series," in *2019 IEEE International Conference on Big Data (Big Data)*. IEEE, 2019, pp. 3285–3292.

[13] A. Govindaram and A. Jegatheesan, "Enhancing Industrial IoT Security: Utilizing Blockchain-Assisted Deep Federated Learning for Collaborative Intrusion Detection," *Journal of Electrical Systems*, vol. 20, no. 2s, pp. 1345–1363, 2024.

[14] D. Li, D. Han, T.-H. Weng, Z. Zheng, H. Li, H. Liu, A. Castiglione, and K.-C. Li, "Blockchain for Federated Learning toward Secure Distributed Machine Learning Systems: A Systemic Survey," *Soft Computing*, vol. 26, no. 9, pp. 4423–4440, 2022.

[15] A. Aldaej, T. A. Ahanger, and I. Ullah, "Deep Learning-Inspired IoT-IDS Mechanism for Edge Computing Environments," *Sensors*, vol. 23, no. 24, p. 9869, 2023.

[16] D. Preethi and N. Khare, "Performance Evaluation of Shallow Learning Techniques and Deep Neural Network for Cyber Security," in *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*. IEEE, 2020, pp. 1–5.

[17] S. M. S. Bukhari, M. H. Zafar, M. Abou Houran, Z. Qadir, S. K. R. Moosavi, and F. Sanfilippo, "Enhancing Cybersecurity in Edge IIoT Networks: An Asynchronous Federated Learning Approach with a Deep Hybrid Detection Model," *Internet of Things*, p. 101252, 2024.

[18] R. Vinayakumar, K. Soman, and P. Poornachandran, "Applying Convolutional Neural Network for Network Intrusion Detection," in *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. IEEE, 2017, pp. 1222–1228.

[19] M. Azizjon, A. Jumabek, and W. Kim, "1D CNN Based Network Intrusion Detection with Normalization on Imbalanced Data," in *2020 international conference on artificial intelligence in information and communication (ICAIIC)*. IEEE, 2020, pp. 218–224.

[20] T. Xie, W. Ding, J. Zhang, X. Wan, and J. Wang, "Bi-LS-AttM: A Bidirectional LSTM and Attention Mechanism Model for Improving Image Captioning," *Applied Sciences*, vol. 13, no. 13, p. 7916, 2023.

[21] b. Senthil Kumar and N. Malarvizhi, "Bi-Directional LSTM–CNN Combined Method for Sentiment Analysis in Part of Speech Tagging (PoS)," *International Journal of Speech Technology*, vol. 23, pp. 373–380, 2020.

[22] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao, "Federated Learning in Mobile Edge Networks: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2031–2063, 2020.

[23] M. Catillo, A. Pecchia, and U. Villano, "Traditional vs Federated Learning with Deep Autoencoders: A Study in IoT Intrusion Detection," in *2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. IEEE, 2023, pp. 208–215.

[24] W. Ding, M. Abdel-Basset, and R. Mohamed, "DeepAK-IoT: An Effective Deep Learning Model for Cyberattack Detection in IoT Networks," *Information Sciences*, vol. 634, pp. 157–171, 2023.

[25] P. Spadaccino and F. Cuomo, "Intrusion Detection Systems for IoT: Opportunities and Challenges Offered by Edge Computing and Machine Learning," *arXiv Preprint arXiv:2012.01174*, 2020.

[26] B. Omarov, O. Auelbekov, A. Suliman, and A. Zhaxanova, "CNN-BiLSTM Hybrid Model for Network Anomaly Detection in Internet of Things," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 3, 2023. [Online]. Available: http://dx.doi.org/10.14569/IJACSA.2023.0140349

[27] P. Kiss, T. Horváth, and V. Felbab, "Stateful Optimization in Federated Learning of Neural Networks," in *Intelligent Data Engineering and Automated Learning–IDEAL 2020: 21st International Conference, Guimaraes, Portugal, November 4–6, 2020, Proceedings, Part II 21*. Springer, 2020, pp. 348–355.

[28] T. Altaf, X. Wang, W. Ni, G. Yu, R. P. Liu, and R. Braun, "A New Concatenated Multigraph Neural Network for IoT Intrusion Detection," *Internet of Things*, vol. 22, p. 100818, 2023.