JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol XI No 4, September 2025, hlm. 653 – 660 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v11i4.4136
Available online at https://jurnal.stmikroyal.ac.id/index.php/jurteksi

CNN-BASED ADAPTIVE IDS WITH FEDERATED LEARNING FOR IOT NETWORK SECURITY

Sahren[1*], Ruri Ashari Dalimunthe[1], Cecep Maulana [2], Yogi Abimanyu Permana[1]
[1]Computer System, Universitas Royal
[2]Information System, Universitas Royal
email :*sahren.one@gmail.com

Abstract: In the era of the Internet of Things (IoT), cyber threats are increasingly complex and dynamic, thus demanding an adaptive and intelligent network security system. This study proposes a Convolutional Neural Network (CNN)-based Intrusion Detection System (IDS) implemented through a Federated Learning (FL) approach in a Non-Independent and Identically Distributed (Non-IID) data environment. This approach allows the model to be trained in a distributed manner across multiple IoT devices without having to collect sensitive data to a central server, thereby maintaining data privacy while increasing the efficiency of the training process. The experiment used the CIC IoT 2023 dataset, which represents various modern IoT network traffic patterns. The results show that the proposed CNN–FL model achieves an overall accuracy of 0.99, with excellent performance in detecting various types of network traffic. The model obtains a perfect recall value (1.00) for normal traffic (Benign), as well as a very high F1-score for DDoS (0.99) and DoS (0.99) attacks. Stable and consistent performance across all five federation rounds demonstrates that this approach is a reliable, efficient, and accurate solution for detecting threats in distributed and privacy-preserving IoT networks.

Keywords: CNN; federated_learning; IDS; non-iid; ciciot2023

Abstrak: Dalam era Internet of Things (IoT), ancaman siber semakin kompleks dan dinamis, sehingga menuntut sistem keamanan jaringan yang adaptif dan cerdas. Penelitian ini mengusulkan Intrusion Detection System (IDS) berbasis Convolutional Neural Network (CNN) yang diterapkan melalui pendekatan Federated Learning (FL) pada lingkungan data yang bersifat Non-Independent and Identically Distributed (Non-IID). Pendekatan ini memungkinkan model dilatih secara terdistribusi di berbagai perangkat IoT tanpa harus mengumpulkan data sensitif ke server pusat, sehingga mampu menjaga privasi data sekaligus meningkatkan efisiensi proses pelatihan. Eksperimen menggunakan dataset CIC IoT 2023, yang merepresentasikan berbagai pola lalu lintas jaringan IoT modern. Hasil penelitian menunjukkan bahwa model CNN–FL yang diusulkan mencapai akurasi keseluruhan sebesar 0.99, dengan performa yang sangat baik dalam mendeteksi berbagai jenis lalu lintas jaringan. Model memperoleh nilai recall sempurna (1.00) untuk lalu lintas normal (Benign), serta nilai F1-score yang sangat tinggi untuk serangan DDoS (0.99) dan DoS (0.99). Kinerja yang stabil dan konsisten di seluruh lima putaran federasi membuktikan bahwa pendekatan ini merupakan solusi yang andal, efisien, dan akurat untuk mendeteksi ancaman pada jaringan IoT yang bersifat terdistribusi dan menjaga privasi (privacy-preserving).

Kata kunci: CNN; federated_learning; IDS; non-iid; ciciot2023

INTRODUCTION

IoT's explosive growth has transformed a number of industries, including digital healthcare, smart transportation, and Industry 4.0 [1]. But as IoT adoption has grown, the attack surface [2] has also expanded, leaving

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol XI No 4, September 2025, hlm. 653 – 660 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v11i4.4136
Available online at https://jurnal.stmikroyal.ac.id/index.php/jurteksi

IoT devices extremely susceptible to DoS, MITM, and SQL injection attacks, among other cyberthreats [3]. The lack of integrated security systems and the constrained computing and communication capabilities of IoT devices make this worse [4]. As a remedy, convolutional neural network (CNN)-based deep learning techniques have demonstrated high performance in identifying cyberattack patterns [5].

CNNs outperform conventional techniques in detecting attacks and identifying intricate aspects of network traffic [6] [7]. The Intrusion Detection System (IDS) is a popular method for detecting attacks [8] [9]. Despite their widespread use, machine learning-based intrusion detection systems still have drawbacks, including a reliance on central servers [10], an inability to manage dispersed non-IID data, and the possibility of data privacy breaches when data is sent to servers for analysis [6] [11].

In the meantime, deep learning techniques in particular, CNNs have shown promise in identifying intricate attack patterns [12]. However, the privacy and decentralization features of traditional CNN models are still restricted [13]. The purpose of this research is to design and implement an intrusion detection system based on Convolutional Neural Network (CNN) with Federated Learning (FL) to overcome the problems of data privacy, centralization, and computational limitations in IoT devices, while maintaining high detection accuracy.

Several related studies have been conducted, [12] "A Federated Learning-Based Approach to Improve Intrusion Detection in Industrial IoT Networks," focuses on the use of FL to detect intrusions in Industrial IoT (IIoT). The study found that FL can achieve nearly equivalent performance to centralized machine learning without the need for raw data sharing. However, the study did not implement a more complex CNN architecture into FL.

"Federated Learning for IoT Intrusion Detection" [13]. examines a number of aggregation methods, including FedAvg, FedAvgM, FedAdam, and FedAdagrad, and uses ANN models to assess FL in IoT IDS. The findings demonstrate that FedAvg offers the greatest outcomes across a range of situations. This study does not specifically address attack mitigation in FL-based CNN contexts, and it currently lacks a precise plan for managing non-IID data in IoT networks.

The study "DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber-Physical Systems" [14]. Instead of concentrating on the particular CNN in the FL combo for IoT IDS, this study creates a Federated Deep Learning model for IDS in Industrial Cyber-Physical Systems. The study [15] "Fleam: A Federated Learning Empowered Architecture to Mitigate DDoS in Industrial IoT". This study looks into federated learning for industrial IoT DDoS attack mitigation, although it hasn't included the CNN approach in its model.

Previous research entitled “Federated learning in intrusion detection: advancements, applications, and future directions” [16] Federated Learning (FL) effectively improves accuracy and preserves data privacy in Intrusion Detection Systems (IDS) through distributed training. Models like FEDGAN-IDS and FedAGRU reach up to 99% accuracy on datasets such as NSL-KDD, UNSW-NB15, and CICIDS2017, even under non-IID

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol XI No 4, September 2025, hlm. 653 – 660 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v11i4.4136
Available online at https://jurnal.stmikroyal.ac.id/index.php/jurteksi

conditions. Hybrid methods like CNN-LSTM and DeepFed (CNN+GRU) also excel in IoT attack detection. Nonetheless, challenges with non-IID data, communication efficiency, and attack resilience require further research for optimal IoT-based IDS implementation.

The research entitled "Designing Homomorphic Encryption-Based Federated Learning for Internet of Things Devices" [17]. This study designs Homomorphic Encryption-based Federated Learning (FHL) to enhance data security in IoT devices. Each device performs local training without sharing raw data, while protecting information during global aggregation. Using logistic regression for binary classification, the research compares conventional FL with FL integrated with FHL. Results show FHL slightly reduces accuracy (0.2–3.4%) due to polynomial approximation of the sigmoid function, but as sample size increases, the gap narrows. Thus, FHL effectively strengthens privacy protection with minimal impact on performance.

A recent study titled "Decentralized AI on The Edge: Implementing Federated Learning for Predictive Maintenance in Industrial IoT Systems" explores using Federated Learning (FL) within Edge AI systems for predictive maintenance in Industrial IoT (IIoT) environments. This research developed a decentralized AI framework running on low-power embedded devices (like ARM Cortex-M) with sensors to detect machine anomalies in real time without transmitting raw data to a central server. Experiments demonstrated significant improvements over centralized systems, including anomaly detection accuracy up to 91.8%, 11.3% better memory efficiency, and 23.6% lower latency. Furthermore, using kernel isolation and Rust-based programming enhanced security against cyberattacks. This confirms that integrating FL and Edge AI on embedded devices is a feasible, efficient, privacy-preserving, and scalable solution for Industry 4.0 predictive maintenance systems [18].

Based on the results analyzed from various previous studies, it can be concluded that although Federated Learning (FL) has been widely applied in the development of Internet of Things (IoT) based Intrusion Detection Systems (IDS), most studies still have limitations in terms of model architecture adaptability, handling of Non-IID data, and resilience to attacks in a federated environment. Some studies, such as [12] and [13], show that FL is able to achieve performance close to centralized learning, but still use simple models such as ANN and have not integrated complex CNN architectures to handle IoT data heterogeneity. Other studies, such as [14] and [15] do propose deep federated models, but do not specifically focus on the combination of CNNs in the context of IoT-based IDS.

In addition, studies [16] and [17] successfully improve data privacy using the Homomorphic Encryption approach and various federation mechanisms, but have not optimized the adaptive CNN architecture to address the distribution of Non-IID data that is common in IoT networks. Meanwhile, research [18] is more oriented towards implementing FL for predictive maintenance in Industrial IoT, rather than intrusion detection systems. Thus, a major gap that has not been filled by much previous research is the need for an adaptive CNN-FL model that is not only able to address class imbalance and non-IID data distribution, but also maintains high accuracy and

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol XI No 4, September 2025, hlm. 653 – 660 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v11i4.4136
Available online at https://jurnal.stmikroyal.ac.id/index.php/jurteksi

convergence stability in distributed IoT environments.

The novelty of this research lies in the development of a CNN-based Intrusion Detection System (IDS) integrated with adaptive Federated Learning to address the key challenges of IoT networks, namely class imbalance, non-IID data, and device computational limitations. This research combines advanced data preprocessing strategies (SMOTE, class weighting, redundant feature elimination) with an adaptive CNN architecture, on the CIC IoT 2023 dataset [3], and applies a FL mechanism that preserves local data privacy and global model convergence stability. This approach makes a significant contribution in delivering an adaptive, effective, and privacy-preserving IDS that is ready to be implemented in large-scale IoT ecosystems.

METHOD

The methodology consists of five main stages: dataset preparation, preprocessing, CNN model design, federated training, and evaluation. The experiment utilizes the CIC IoT 2023 dataset, which contains both benign traffic and various types of attack scenarios such as Denial of Service (DoS) and Distributed Denial of Service (DDoS). This dataset is highly suitable because it reflects real-world IoT traffic patterns in contemporary network environments.

The experimental implementation was conducted on a system running Windows 11 Pro with a Ryzen 7 processor, AMD GPU (8 GB VRAM), 1 TB storage, and Python 3.11 as the programming environment. The deep learning models were developed using the PyTorch framework (version 2.8.0), which supports efficient computation for CNN-based architectures and federated learning simulations.

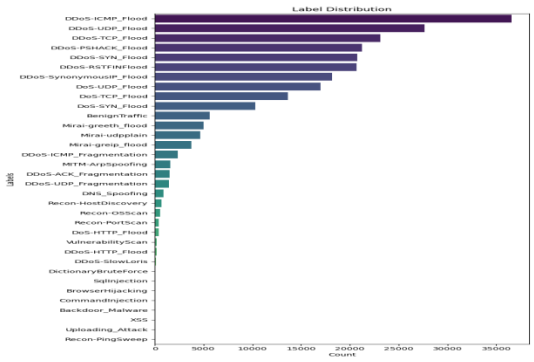

Image 1. Label Distribution Dataset

The CIC IoT 2023 dataset displays a strong class imbalance, with DDoS attack types (like ICMP, UDP, and TCP Floods) dominating, while categories such as Reconnaissance, XSS, and Uploading_Attack are significantly underrepresented. To mitigate this, SMOTE (Synthetic Minority Oversampling Technique) was applied to enhance minority class representation. Before training, numerical features were normalized to the [0,1] range for consistent learning, and the dataset was partitioned across multiple clients to simulate the heterogeneous and non-IID distributions typical of real-world IoT environments.

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

This research employs a CNN-LSTM architecture to classify IoT traffic as Benign, DoS, or DDoS by capturing spatial and temporal features. The model includes convolutional layers (32 and 64 filters, ReLU) with MaxPooling1D, a 32-unit LSTM, and fully connected layers with ReLU and Softmax for classification. Federated Learning (FL) is applied, with local training using Adam

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol XI No 4, September 2025, hlm. 653 – 660 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v11i4.4136
Available online at https://jurnal.stmikroyal.ac.id/index.php/jurteksi

(lr=0.001), CrossEntropyLoss, batch size 64, and 20 epochs. Client weights are aggregated via FedAvg over five communication rounds with secure aggregation. The PI designed the architecture and FL setup, while the AI handled implementation, local training, and aggregation

The effectiveness of the proposed IDS is measured using standard classification metrics:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (2)$$

$$\text{Precision} = \frac{TP}{TP+FP} \quad (3)$$

$$\text{Recall} = \frac{TP}{TP+FN} \quad (4)$$

$$\text{F1-Score} = \frac{2*\text{Precision}*\text{Recall}}{\text{Precision}+\text{Recall}} \quad (5)$$

RESULT AND DISCUSSION

The dataset used faced challenges related to imbalanced data, so during dataset preparation, an imbalance process was performed using oversampling (SMOTE) or undersampling and class weights. As seen in Figure 2 below, this procedure grouped the dataset's labels:

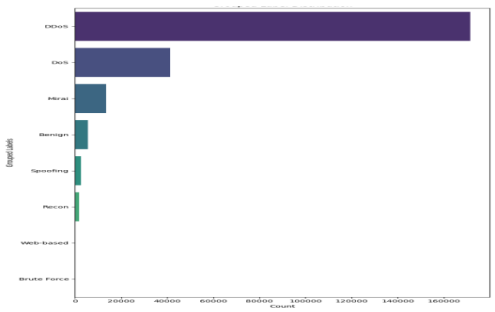

Image 2. Group Label Distribution

The Different Image 1, Image 2 groups labels into benign, DoS, and DDoS. Besides grouping, feature removal is applied to optimize the model by eliminating redundancy. From highly correlated pairs, one feature is retained—for example, keeping Rate over Srate, IPv over LLC, and retaining Number, AVG, and Std instead of Weight, Magnitude, and Radius. Total-based features like Tot sum and Tot size are replaced with AVG, with PCA as an alternative. The fin_flag_number feature is also removed, while ack_count is kept to simplify protocol representation. This approach cleans data, reduces complexity, and improves training efficiency without losing essential information, resulting in better performance and interpretability.

In data analysis, inefficient data types often waste memory and slow computation. For instance, float64 is used to store Boolean flags (0/1) and protocol indicators (e.g., HTTP, HTTPS), which is unnecessary. The solution is twofold: convert flag columns to compact types like uint8 (1 byte vs. 8 bytes), and convert protocol/service columns to categorical types, which store repeated values efficiently. These optimizations improve memory usage and speed up analysis, creating a more efficient workflow

Imbalance in feature scales is a common issue that can impact model performance. Based on the evidence provided, features such as Covariance (with a maximum value of 1.37×10^{8}) and Weight (with a maximum value of 244) have very different value ranges.

The CIC IoT 2023 dataset [3] was used to successfully train an Intrusion Detection System (IDS) based on Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) within a Federated Learning framework. Three clients participated in the experiment's five rounds (federated rounds), with each client using a distinct subset of data to train its local model. A

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol XI No 4, September 2025, hlm. 653 – 660 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v11i4.4136
Available online at https://jurnal.stmikroyal.ac.id/index.php/jurteksi

global model was then created by combining the model weights.

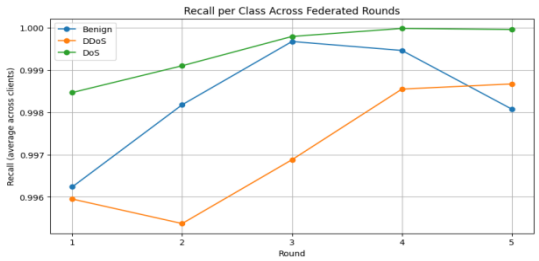

Image 3. Average Recall per Class Per Round (Federate Learning)

The average recall per class across five Federated Learning (FL) rounds, highlighting the consistency and robustness of the CNN model in classifying IoT network traffic. The Benign class achieved a perfect recall of 1.000 in multiple rounds, indicating that the model was able to correctly identify all normal traffic samples without misclassification. Meanwhile, the DoS class maintained the highest and most stable recall performance, consistently reaching 1.000 after the third round, demonstrating the model's strong ability to detect DoS attacks accurately.

The DDoS class, although showing a slight fluctuation in earlier rounds, stabilized above 0.998 by the final round, reflecting excellent generalization and adaptability throughout the federated training process. Overall, these results confirm that the model remains highly stable and reliable during successive FL rounds, successfully maintaining detection performance across all traffic classes and ensuring robust intrusion detection in IoT network environments.

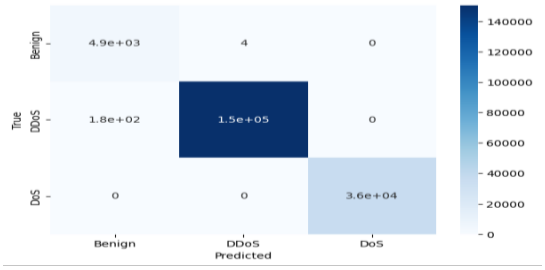

Image 4. Confusion Matrix Global Model CCN With Federated Learning

Based on the Confusion Matrix in Figure 4, a global CNN model utilizing Federated Learning (FL) demonstrated exceptional performance in detecting three classes of IoT network traffic: Benign, DDoS, and DoS. The model achieved a very high accuracy, particularly in the DoS class where all 36,000 samples were correctly classified. In the Benign class, 4,900 samples were correct with only 4 misclassified as DDoS, and for the DDoS class, approximately 150,000 samples were correctly predicted with only about 180 misclassified as Benign.

The overall very low misclassification rate across all classes confirms that the FL-based CNN model is reliable, stable, and highly effective for Intrusion Detection Systems (IDS) in distributed IoT environments, successfully distinguishing between normal traffic and major attacks like DDoS and DoS, as further supported by the full Global Evaluation metrics.

Table 1. Global Evaluation

	Precision	Recall	F1-score	Support
Benign	0.97	1.00	0.98	4895
DDoS	0,99	1.00	0.98	150661
DoS	0,99	1.00	0.98	36296
accuracy			0,99	191852
macro avg	0.99	1.00	0.99	191852

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol XI No 4, September 2025, hlm. 653 – 660 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v11i4.4136
Available online at https://jurnal.stmikroyal.ac.id/index.php/jurteksi

weighted avg	1.00	1.00	1.00	191852

With an overall accuracy of 0.99, Table 1 shows that the proposed CNN model trained with Federated Learning (FL) achieves highly reliable performance across all traffic categories. Metrics for Benign, DDoS, and DoS classes confirm balanced accuracy: the Benign class reached recall 1.00 (perfect detection of normal traffic) with precision 0.97 and F1-score 0.98; the DDoS class obtained precision 0.99, recall 1.00, and F1-score 0.98; while the DoS class achieved precision 0.99, recall 1.00, and F1-score 0.99. These results highlight the model's strong capability in accurately identifying different IoT network traffic types with minimal errors.

Furthermore, the macro average (precision 0.99, recall 1.00, f1-score 0.99) confirms that the model performs consistently across all classes, regardless of class imbalance. The weighted average (1.00 for all metrics) further validates the model's stability and adaptability under Non-IID data conditions. Overall, these results confirm that the Federated CNN model is a highly dependable and effective IDS solution for detecting both benign and malicious traffic in distributed IoT network environments.

CONCLUSION

The CIC IoT 2023 dataset faced severe class imbalance, mitigated with class weights, SMOTE, and undersampling, while labels were grouped into Benign, DoS, and DDoS. Model optimization—through feature reduction, categorical encoding, and normalization—enhanced CNN performance. In a Federated Learning (FL) setup, the model achieved 0.99 accuracy, 0.99 macro average, and 1.00 weighted average, with perfect recall for Benign traffic and low error rates for DoS/DDoS. The federated architecture effectively managed non-IID data, ensuring stable convergence and balanced client performance. Practically, the CNN–FL IDS can run on edge devices or IoT gateways for real-time, privacy-preserving detection, making it scalable and secure for smart cities, industrial IoT, and critical infrastructures.

BIBLIOGRAPHY

[1] S. Hirmansyah Siregar, R. Yesputra, P. Studi Sistem Komputer, and S. Royal, "Automatic Security System In Bhayangkara Indah Office From Theft, Gas Leakage, And Fire And Flood Based On Arduino Nano," *J. Tek. Inform.*, vol. 3, no. 3, pp. 689–695, 2022, [Online]. Available: https://doi.org/10.20884/1.jutif.2022.3.3.261

[2] N. Ariana, S. Mandala, M. F. Hassan, M. Qomaruddin, and B. Ibrahim, "Intrusion Detection System Development on Internet of Things using Ensemble Learning," vol. 2, 2024.

[3] 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, 2023, doi: 10.3390/s23135941.

[4] J. N. Sibarani, D. R. Sirait, and S. S. Ramadhanti, "Intrusion Detection Systems pada Bot-IoT Dataset Menggunakan Algoritma Machine Learning," *J. Masy. Inform.*, vol. 14, no. 1, pp. 38–52, 2023, doi: 10.14710/jmasif.14.1.49721.

[5] S. Sahren and L. Adi, Prijuna,

"Intrusion Detection System Berbasis Deep Learning Untuk Peningkatan Mitigasi Sql Injection," vol. 4307, no. 4, pp. 1866–1874, 2024.

[6] S. Mandala, W. Jatmiko, S. Nurmaini, A. Rizal, and Adiwijaya, "OCADN: Improving Accuracy in Multi-class Arrhythmia Detection from ECG Signals with a Hyperparameter-Optimized CNN," *IEEE Access*, vol. 13, no. December 2024, pp. 34687–34705, 2025, doi: 10.1109/ACCESS.2025.3544273.

[7] A. Harshavardhan, M. Sree Vani, A. Patil, N. Yamsani, and K. Archana, "Hybrid Deep Learning Framework for Intrusion Detection: Integrating Cnn, Lstm, and Attention Mechanisms To Enhance Cybersecurity," *J. Theor. Appl. Inf. Technol.*, vol. 103, no. 1, pp. 63–78, 2025.

[8] S. Sahren, R. A. Dalimunthe, H. Saputra, and D. Y. Kurnia Sirni, "Idps Performance Analysis for Mitigating Sql Injections and Syn Flood Attacks," *JURTEKSI (Jurnal Teknol. dan Sist. Informasi)*, vol. 10, no. 1, pp. 171–178, 2023, doi: 10.33330/jurteksi.v10i1.2880.

[9] Q. Li, Y. Diao, Q. Chen, and B. He, "Federated Learning on Non-IID Data Silos: An Experimental Study," *Proc. - Int. Conf. Data Eng.*, vol. 2022-May, pp. 965–978, 2022, doi: 10.1109/ICDE53745.2022.00077.

[10] M. R. Wijaya, "Inovasi Model Intrusion Detection System (IDS) menggunakan Double Layer Gated Recurrent Unit (GRU) dengan Fitur Berbasis Fusion," vol. 12, no. 1, pp. 10–21, 2025.

[11] Weny Indah Kusumawati and Adisaputra Zidha Noorizki, "Perbandingan Performa Algoritma VGG16 Dan VGG19 Melalui Metode CNN Untuk Klasifikasi Varietas Beras," *J. Comput. Electron. Telecommun.*, vol. 4, no. 2, 2023, doi: 10.52435/complete.v4i2.387.

[12] M. M. Rashid, S. U. Khan, F. Eusufzai, M. A. Redwan, S. R. Sabuj, and M. Elsharief, "A Federated Learning-Based Approach for Improving Intrusion Detection in Industrial Internet of Things Networks," *Network*, vol. 3, no. 1, pp. 158–179, 2023, doi: 10.3390/network3010008.

[13] R. Lazzarini, H. Tianfield, and V. Charissis, "Federated Learning for IoT Intrusion Detection," *AI*, vol. 4, no. 3, pp. 509–530, 2023, doi: 10.3390/ai4030028.

[14] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber-Physical Systems," *IEEE Trans. Ind. Informatics*, vol. 17, no. 8, pp. 5615–5624, 2021, doi: 10.1109/TII.2020.3023430.

[15] J. Li, L. Lyu, X. Liu, X. Zhang, and X. Lyu, "FLEAM: A Federated Learning Empowered Architecture to Mitigate DDoS in Industrial IoT," *IEEE Trans. Ind. Informatics*, vol. 18, no. 6, pp. 4059–4068, 2022, doi: 10.1109/TII.2021.3088938.

[16] B. Buyuktanir, Ş. Altinkaya, G. Karatas Baydogmus, and K. Yildiz, "Federated learning in intrusion detection: advancements, applications, and future directions," *Cluster Comput.*, vol. 28, no. 7, 2025, doi: 10.1007/s10586-025-05325-w.

[17] Y. M. Saputra, G. Alfian, and M. Q. H. Octava, "Perancangan Federated Learning Berbasis Homomorphic Encryption untuk Perangkat Internet of Things," *J. Internet Softw. Eng.*, vol. 4, no. 1, pp. 1–5, 2023, doi: 10.22146/jise.v4i1.6378.

[18] C. Supriadi, W. Wahyudi, A. Priyadi, and K. S. Jin, "Decentralized AI on The Edge : Implementing Federated Learning for Predictive Maintenance in Industrial IoT Systems," vol. 4, no. 2, pp. 317–334, 2025.