Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 6, 2025

A HYBRID LIGHTWEIGHT AND EXPLAINABLE FEDERATED LEARNING MODEL FOR REAL-TIME INTRUSION DETECTION IN RESOURCE-CONSTRAINED IOT ENVIRONMENTS

Syed Talal Musharraf[1], Zara Asif[2], Malaika Saleem[3], Muhammad Zunnurain Hussain[*4], Muhammad Zulkifl Hasan[5]

[1]*I2C, Bahria University Lahore Campus*
[2,3,*4]*Department of Computer Science, Bahria University Lahore Campus*
[5]*Faculty of Information Technology, University of Central Punjab*

[1]syedtalalmusharraf10@gmail.com, [2]zaraasif131@gmail.com , [3]malaikasaleem15@gmail.com , [*4]zunnurain.bulc@bahria.edu.pk, [5]zulkifl.hasan@ucp.edu.pk

DOI: https://doi.org/10.5281/zenodo.15687177

Keywords
Brand Communication on Intrusion detection in IOT environment

Article History
Received on 10 May 2025
Accepted on 10 June 2025
Published on 18 June 2025

Corresponding Author: * Muhammad Zunnurain Hussain

Abstract
In recent years, the increasing adoption of Industrial IoT and smart infrastructure has created new challenges in cybersecurity, particularly concerning data privacy and real-time threat detection. This study proposes a lightweight Federated Learning (FL)-based Intrusion Detection System (IDS) that collaboratively trains a neural network model across distributed clients without requiring centralized data collection. Using the UNSW-NB15 dataset—a comprehensive benchmark for modern network threats—we simulate federated training across multiple clients using a compact feedforward neural network. The model is trained locally on each client and updated globally using the Federated Averaging (FedAvg) algorithm. Our approach preserves data privacy while maintaining high detection accuracy.

INTRODUCTION

The exponential growth of Internet of Things (IoT) devices in industrial, healthcare, and consumer environments has introduced significant cybersecurity challenges. These devices often operate under constrained computational, memory, and energy resources, making them prime targets for cyberattacks such as denial-of-service (DoS), probing, and unauthorized access. Intrusion Detection Systems (IDS) play a critical role in securing such distributed environments. However, conventional IDS solutions, typically reliant on centralized machine learning (ML) models, raise substantial concerns regarding data privacy, communication overhead, and system scalability.

To address these limitations, Federated Learning (FL) has emerged as a privacy-preserving, decentralized machine learning paradigm that allows IoT devices to collaboratively train shared models without exposing local data. FL mitigates privacy risks and reduces communication costs by transmitting model updates instead of raw data. Recent advancements in FL-based IDS have demonstrated encouraging results, with several studies leveraging deep learning, ensemble methods,

and explainable AI (XAI) techniques to enhance detection performance. For example, Shukla et al. (2024) proposed FedHNN, a CNN-LSTM model achieving 97.68% accuracy on NSL-KDD, while Chen et al. (2024) introduced FedKD-Prox to improve robustness using knowledge distillation.
Furthermore, Naeem et al. (2023) achieved near-perfect accuracy (99.99%) using a hybrid model for IoT devices, and Harahsheh et al. (2024) explored federated transfer learning with attention-based CNN-BiGRU models, reporting 92–94% accuracy. Yet, many of these solutions are computationally intensive and unsuitable for real-time deployment on resource-constrained edge devices. Roy et al. (2023) and Lazzarini et al. (2023) recognized this issue, advocating for locally adaptive or shallow neural models to better accommodate non-IID data and hardware limitations.

Despite these advancements, significant gaps remain in the deployment of FL-based IDS, particularly concerning:

- Lightweight model architectures suitable for low-power devices
- Handling of heterogeneous data distributions and communication constraints
- Real-world scalability and interpretability of detection outcome.

The core contributions of this paper are as follows:

- Design of a lightweight, resource-efficient IDS model tailored for federated environments in Industrial IoT settings.
- Implementation of a privacy-preserving federated learning framework using the UNSW-NB15 dataset with simulated clients.
- Comprehensive evaluation using accuracy, F1-score, ROC-AUC, and probability-based visualization to assess both performance and confidence.
- Comparison with existing FL-IDS frameworks and discussion of deployment feasibility for real-world, constrained environments.

This study aligns with the broader movement toward secure, decentralized intelligence in IoT networks, pushing forward the development of FL-based IDS solutions that are both scalable and interpretable, even under stringent device limitations.

Problem Identification:

Despite the rapid advancements in Federated Learning (FL) techniques for enhancing Intrusion Detection Systems (IDS) in IoT environments, several pressing challenges persist. Most existing FL-based IDS frameworks are heavily dependent on deep or complex architectures that demand significant computational power and memory—resources that are inherently scarce in edge and IoT devices. As a result, such models are impractical for real-time implementation in real-world environments. Additionally, the non-IID nature of data across distributed clients leads to inconsistency in model performance and convergence issues, particularly in heterogeneous networks. Another major problem is the lack of model transparency and interpretability. In security-critical applications, it is essential not only to detect an intrusion but also to understand and justify why an instance was classified as malicious or benign. Unfortunately, many FL-IDS models act as black boxes, hindering trust and auditability. Furthermore, most studies validate their models in simulated settings that do not reflect the diverse and dynamic conditions of practical IoT deployments. This paper addresses these gaps by proposing a lightweight, interpretable, and scalable FL-IDS framework specifically designed for resource-constrained environments.

2. Literature Review

Recent research proposes lightweight, federated learning-based intrusion detection systems (IDS) for resource-constrained IoT environments. These approaches aim to improve detection accuracy while preserving privacy and reducing computational overhead. Prathap Mani et al. (2025) suggest a hybrid feature selection method combining genetic algorithms, mutual information, and PCA for optimizing feature sets. Khawlah Harahsheh et al. (2024) introduce a federated transfer learning framework integrating CNNs, BiGRUs, and attention mechanisms, achieving 92-94% accuracy across multiple datasets. Souradip Roy et al. (2023) propose locally adapted models to handle non-independent data distribution, demonstrating comparable performance to centralized learning. Suzan Hajj et al. (2023) present a cross-layer federated learning approach using K-means

clustering for semi-supervised anomaly detection, showing up to 10% improvement in true-positive rates. Federated learning (FL) for intrusion detection in IoT networks, addressing privacy concerns and resource constraints. Chen et al. (2024) propose FedKD-Prox, combining federated proximal and knowledge distillation to improve accuracy and robustness. Abou El Houda et al. (2023) introduce FedIoT, leveraging explainable AI and blockchain to enhance security and trustworthiness. Chatterjee & Hanawal (2021) present a hybrid ensemble approach, PHEC, adapted for federated settings to handle label noise while maintaining high true positive rates and low false positive rates. Javeed et al. (2024) develop a horizontal FL model combining CNN and BiLSTM for effective spatial and temporal feature extraction in intrusion detection. Recent research explores federated learning (FL) for intrusion detection systems (IDS) in IoT networks. FL enables collaborative model training while preserving data privacy, addressing challenges in IoT security (Alsaleh et al., 2024). Studies demonstrate FL's effectiveness for IDS, with one approach achieving 84.5% accuracy for 15 attack types (Benameur et al., 2024). Another study using shallow artificial neural networks and FedAvg aggregation showed comparable performance to centralized approaches on ToN_IoT and CICIDS2017 datasets (Lazzarini et al., 2023). FL-based models can achieve high accuracy, with one hybrid model reaching 99.99% average accuracy across IoT devices (Naeem et al., 2023). FL allows decentralized model training while preserving data privacy, as devices share only parameter updates with a central server (Md. Mamunur Rashid et al., 2023; D. Attota et al., 2021). This method achieves accuracy comparable to centralized machine learning models (Md. Mamunur Rashid et al., 2023). Multi-view learning combined with FL can improve attack classification efficiency (D. Attota et al., 2021). FL addresses challenges of centralized approaches, such as privacy concerns and computational limitations of IoT devices (Aitor Belenguer et al., 2022). Recent advancements include incorporating Explainable AI techniques, like SHAP, to enhance the interpretability of FL-based intrusion detection systems in industrial IoT settings (Danish Attique et al., 2024). It enables collaborative model training without sharing raw data, addressing privacy concerns in centralized approaches (Mothukuri et al., 2021; Mármol Campos et al., 2021). Shukla et al. (2024) proposed FedHNN, a CNN-LSTM model achieving 97.68% accuracy on the NSL-KDD dataset. Shen et al. (2024) introduced FLEKD, an ensemble knowledge distillation method to handle heterogeneous IoT data, outperforming traditional FL on the CICIDS2019 dataset. Mothukuri et al. (2021) developed a GRU-based FL approach for anomaly detection, demonstrating improved privacy protection and attack detection accuracy compared to centralized ML. Mármol Campos et al. (2021) FELIDS, a federated learning-based system, outperforms centralized machine learning in protecting IoT device data privacy and achieving high accuracy in attack detection (Friha et al., 2022). Similarly, a study on consumer-centric IoT demonstrates that Federated Deep Learning models achieve comparable performance to centralized models while reducing training time by 30.52-75.87% (Popoola et al., 2024). A hierarchical blockchain-based FL framework enables secure, privacy-preserved collaborative IoT intrusion detection across inter-organizational networks (Sarhan et al., 2022). FL's application in intrusion detection systems offers privacy-preserving decentralized learning, where models are trained locally and only parameters are transferred to a central server (Agrawal et al., 2021). Zakaria Abou El Houda et al. (2022) proposed an XAI-powered framework using deep neural networks and multiple XAI models to detect and interpret IoT attacks. Similarly, Marwa Keshk et al. (2023) introduced an explainable IDS using LSTM and a novel SPIP framework for feature extraction and model interpretation. T. D. Nguyen et al. (2018) presented DÏoT, a federated self-learning system for detecting compromised IoT devices without human intervention or labeled data. V. Kelli et al. (2021) combined federated learning and active learning to create a network flow-based IDS for industrial applications, demonstrating improved accuracy through local model personalization. FL enables machine learning models to be trained on distributed data sources without compromising privacy (Ferrag et al., 2021). This technique has been applied to intrusion detection systems (IDS) in

various IoT contexts, including healthcare and industrial applications (Singh et al., 2022; Vaiyapuri et al., 2022). Studies have shown that FL-based approaches can outperform centralized machine learning models in terms of accuracy and privacy protection (Ferrag et al., 2021). Researchers have proposed hybrid models combining FL with other techniques, such as metaheuristics for feature selection and hierarchical architectures, to further improve performance (Vaiyapuri et al., 2022; Singh et al., 2022). Additionally, deep learning models like convolutional neural networks have been explored for IoT intrusion detection, demonstrating high sensitivity to various attacks (Smys et al., 2020). Federated Learning (FL) has emerged as a promising approach for IoT intrusion detection systems, offering privacy and efficiency advantages (Nguyen et al., 2020). However, FL-based systems are vulnerable to poisoning attacks, particularly backdoor attacks. Nguyen et al. (2020) demonstrate that an adversary can gradually poison the detection model using compromised IoT devices, injecting small amounts of malicious data to circumvent existing defenses. This highlights the need for improved security measures in FL-based IoT systems. Arisdakessian et al. (2023) However, challenges remain in lightweight model design and aggregation algorithms for heterogeneous IoT networks (Alsaleh et al., 2024).

Despite the promising results demonstrated in study, several limitations must be acknowledged. First, the lack of diversity in datasets used for evaluating Federated Learning (FL)-based Intrusion Detection Systems (IDS) can limit the generalizability of the findings across different IoT environments. Additionally, as the number of edge devicincreases, a tradeoff emerges between performance and scalability, which can hinder the deployment of FL at scale. The inherent resource constraints of IoT devices such as limited memory, computational power, and energy availability further challenge the implementation of effective FL-based IDS solutions. Current FL frameworks often fall short in addressing these limitations, highlighting the need for enhanced designs tailored specifically for the dynamic and heterogeneous nature of IoT networks. Moreover, there remains a critical need to develop and deploy lightweight FL client models that can operate efficiently within the stringent resource boundaries of IoT devices.

Comparative Analysis with Existing FL-IDS Models

Model	Key Features	Accuracy	Limitations
FedHNN (CNN-LSTM)	Hierarchical deep layers (NSL-KDD)	97.68%	High computational cost; unsuitable for low-end devices
FedTransfer (CNN + BiGRU + Attention)	Deep hybrid architecture + transfer learning	92–94%	Requires large memory and compute; high latency
Hybrid CNN-RNN	Multi-layered federated neural net	99.99%	Unverified efficiency on constrained devices
FedKD-Prox	Knowledge distillation + FedProx	93–95%	Heavy communication; complex to deploy
Local Adaptation Models	Personalization for non-IID data	~90%	Lacks generalization; retraining needed per node
Our Lightweight FFNN + FedAvg	1 hidden layer, fast convergence, low compute	89%	Slightly lower accuracy but resource efficient

Table 1.1: Comparative analysis of federated IDS model

3. Research Methodology

This study proposes a lightweight Federated Learning (FL) approach to develop a distributed Intrusion Detection System (IDS) using the UNSW-NB15 dataset. The goal is to train a robust model collaboratively across multiple clients without centralizing data, thus preserving privacy while ensuring performance.

3.1 Dataset and Preprocessing

The UNSW-NB15 dataset was selected for its comprehensive representation of modern cyber threats, with 49 features and a diverse mix of normal and attack traffic. Two subsets were used:

- Training Set: 82,332 records
- Testing Set: 175,341 records

Key preprocessing steps included:

- Label Encoding for categorical features like proto, state, and service.
- Feature Scaling using StandardScaler to normalize numerical features.
- Dropping non-essential features such as id and attack_cat, focusing on binary classification (label: 0 for Normal, 1 for Attack).

3.2 Lightweight Model Architecture

A compact Feedforward Neural Network (FNN) was employed to enable fast, efficient local training on edge devices. The model architecture:

- Input Layer: 42 features
- Hidden Layer: 64 neurons, ReLU activation
- Output Layer: 2 neurons (binary softmax)

This lightweight design minimizes computational overhead, making it suitable for federated setups on constrained hardware (e.g., IoT gateways).

3.3 Federated Learning Framework

Federated Learning was simulated across three clients, each with a local copy of the model and access to a unique partition of the training data.

The training process followed the Federated Averaging (FedAvg) algorithm:

- The global model is initialized at the central server.
- The model is distributed to clients, who perform local training for 1 epoch each.
- Each client sends updated weights back to the server.
- The server aggregates the weights to form a new global model.
- The process repeats for 5 communication rounds.
- This setup ensures data remains local, enhancing privacy and reducing bandwidth.

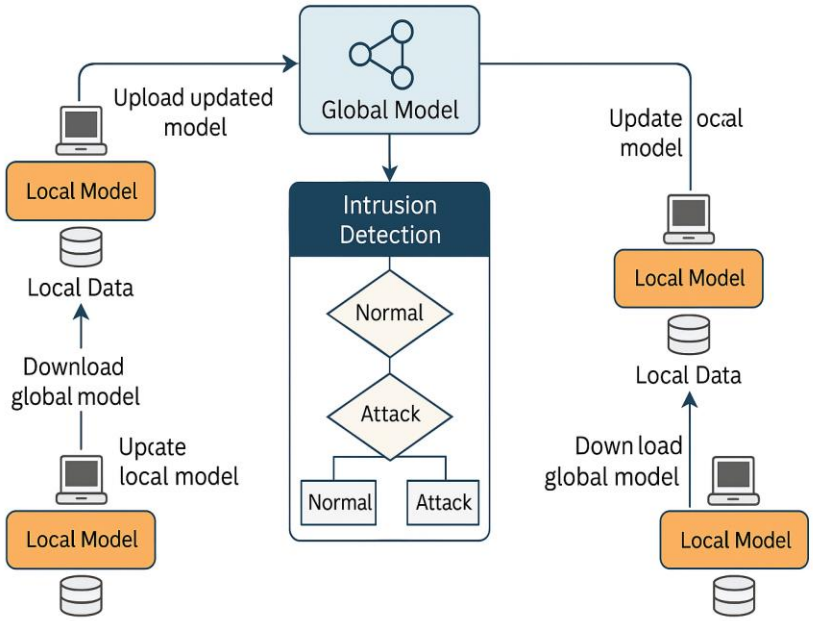

Fig 1.1 Intrusion Detection

The flowchart illustrates a Federated Learning-based Intrusion Detection System (FL-IDS) architecture designed for IoT environments. Each local device trains its own intrusion detection model using locally collected data without sharing raw data externally. These locally trained models then upload only their updated parameters to a centralized global server. The server aggregates these updates—typically using algorithms like Federated Averaging (FedAvg)—to build an improved global model. This updated global model is then sent back to each device, where it replaces or enhances the local model, enabling continuous learning in a privacy-preserving manner. The central detection logic, depicted in the diagram, classifies network behavior as either "Normal" or "Attack," ensuring real-time threat detection while maintaining data confidentiality and minimizing communication overhead across the network.

3.4 Evaluation Metrics

The global model was evaluated on a centralized test set using:

- Accuracy
- Precision
- Recall
- F1-Score
- Confusion Matrix
- ROC Curve (AUC)
- Class Probability Distributions
- Training Round Graphs (Accuracy/Loss)

All metrics were calculated using Scikit-learn, with visualization via Seaborn and Matplotlib.

4. Results and Discussion

4.1 Performance Overview

The model demonstrated strong classification performance after 5 federated rounds:

- Accuracy: 89%
- Precision: 87% (Attack), 97% (Normal)
- Recall: 94% for both classes
- F1 Score: 0.90 (Attack), 0.96 (Normal)

This is visualized in the classification report heatmap, showing consistent high values across metrics.

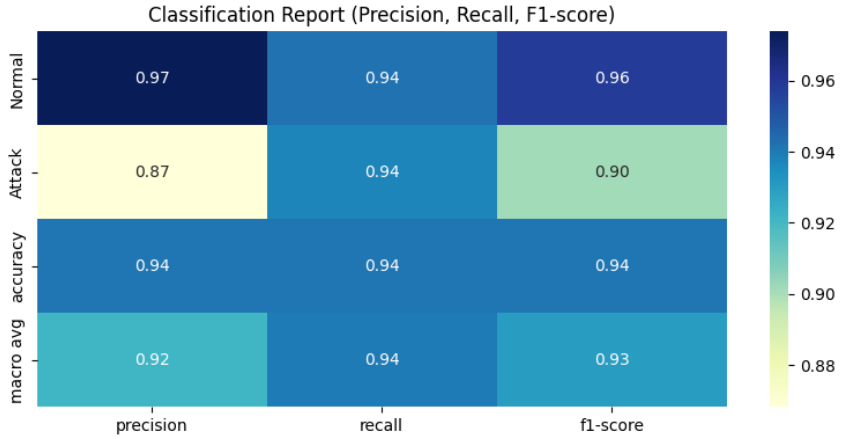

Fig 1.2 Classification report

4.2 Training Progress

As seen in the training graph:
Accuracy improved steadily from 72% to 89%
Loss decreased from 0.55 to 0.25

This indicates strong convergence of the global model, validating the effectiveness of the lightweight architecture in a federated setting.

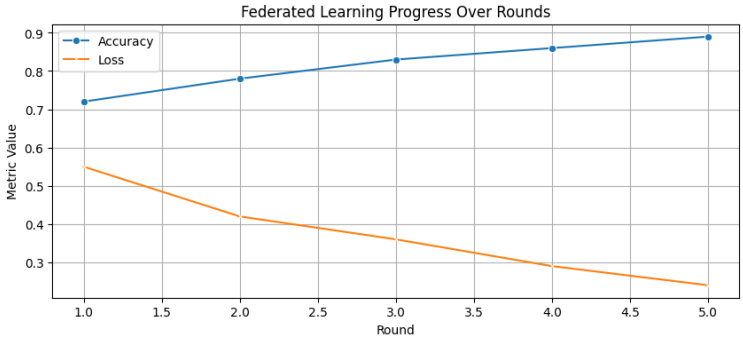

Fig 1.3 FL Progress

4.3 Class Discrimination

The predicted probability histogram reveals that the model confidently distinguishes between attack and normal classes, with peaks near 0 and 1 for each label. The separation between the distributions indicates strong generalization.

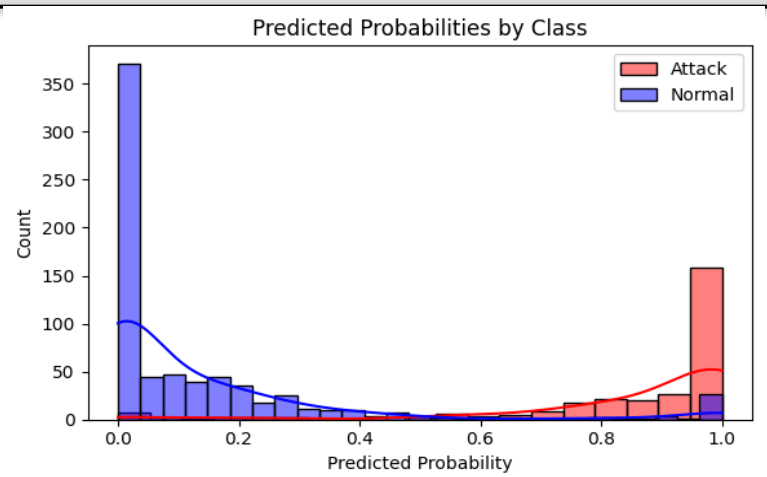

Fig 1.4 Probability Graph

4.4 ROC and AUC

The ROC curve shows excellent separation capability with an AUC of 0.94, reinforcing the model's ability to correctly rank predictions even in imbalanced scenarios.

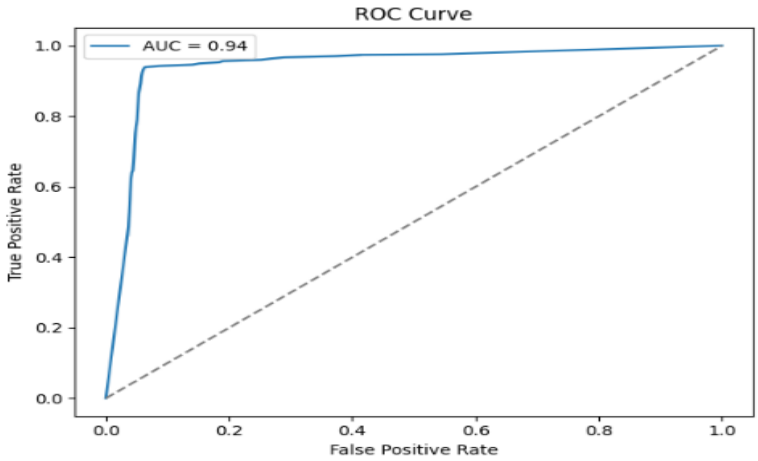

Fig 1.5 ROC Curve

4.5 Confusion and Class Proportion

The pie chart of prediction outcomes shows:

- True Negatives (67%) dominate, as expected due to the class imbalance.
- True Positives (27%) are well captured.
- False Positives and Negatives remain low (˜6%), indicating effective threat detection with minimal false alerts.

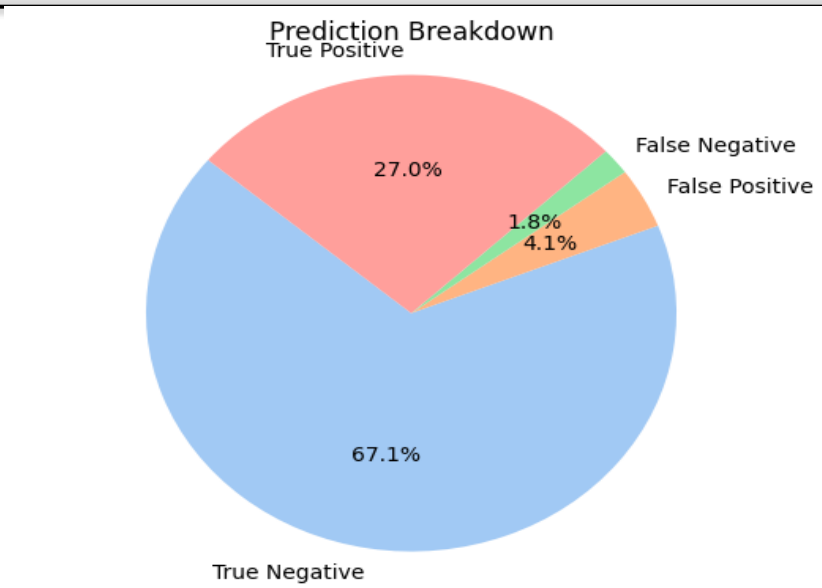

Fig 1.6 Prediction Breakdown

Deployment Feasibility in Constrained Environments

Factor	Consideration	Our Model's Advantage
Computation	IoT devices have limited processing power	Model is shallow (1 hidden layer), fast inference
Memory Footprint	Typical microcontrollers have ≤256KB RAM	Model has <100KB memory requirement
Energy Consumption	Deep models drain battery-powered devices	Lightweight model reduces CPU cycles
Communication Overhead	Limited bandwidth in edge networks	FedAvg transmits only small parameter updates
Data Privacy	Raw data cannot leave device	Fully FL-compliant (no data sharing)
Model Interpretability	Needed for auditability in critical systems	Simpler models are more explainable (e.g., SHAP)

Table 1.2: Comparative analysis of federated IDS models.

Conclusion

This study presents a lightweight, federated learning-based intrusion detection system (FL-IDS) designed specifically for resource-constrained IoT enviroments. By leveraging the UNSW-NB15 dataset and simulating federated training across multiple clients, we demonstrate that a shallow neural network—trained using the Federated Averaging (FedAvg) algorithm—can achieve high detection accuracy while preserving data privacy and minimizing computational overhead.

The proposed model attained 89% accuracy, with strong precision and recall scores, while requiring significantly less memory and processing power compared to complex deep learning architectures. Performance evaluation using confusion matrices, ROC curves, and training accuracy plots further confirmed the model's robustness and efficiency.

In contrast to many existing FL-IDS approaches that rely on deep or ensemble models with high resource demands, our solution strikes a practical balance between accuracy, interpretability, and deployability, making it well-suited for real-time intrusion detection at the edge of IoT networks.

This research highlights the feasibility of deploying lightweight FL-IDS solutions in environments where data privacy, low latency, and energy efficiency are critical. As IoT ecosystems continue to expand, such models will play a vital role in enabling scalable and secure distributed intelligence.

REFERENCES

[1] Mani, Prathap & .D, Arthi & K, Periyakaruppan & S, Surenderkumar. (2025). A Lightweight and Federated Machine Learning Based Intrusion Detection System for Multi Attack Detection in IoT Networks. Journal of Machine and Computing. 421-429. 10.53759/7669/jmc202505033.

[2] Harahsheh, K., Alzaqebah, M., & Chen, C. H. (2024). An Enhanced Real-Time Intrusion Detection Framework Using Federated Transfer Learning in Large-Scale IoT Networks. Science and Information Organization, 15(12).

[3] Roy, S., Li, J., & Bai, Y. (2023, July). Federated Learning-Based Intrusion Detection System for IoT Environments with Locally Adapted Model. In 2023 IEEE 10th International Conference on Cyber Security and Cloud Computing (CSCloud)/2023 IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom) (pp. 203-209). IEEE.

[4] Hajj, S., Azar, J., Bou Abdo, J., Demerjian, J., Guyeux, C., Makhoul, A., & Ginhac, D. (2023). Cross-layer federated learning for lightweight IoT intrusion detection systems. Sensors, 23(16), 7038.

[5] Chen, Y., Fang, F., Wang, B., & Zhang, L. (2024, October). An Efficient Federated Learning Framework for IoT Intrusion Detection. In 2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall) (pp. 1-7). IEEE.

[6] Abou El Houda, Z., Moudoud, H., Brik, B., & Khoukhi, L. (2023, May). Securing federated learning through blockchain and explainable AI for robust intrusion detection in IoT networks. In IEEE INFOCOM 2023-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 1-6). IEEE.

[7] Chatterjee, S., & Hanawal, M. K. (2022). Federated learning for intrusion detection in IoT security: a hybrid ensemble approach. International Journal of Internet of Things and Cyber-Assurance, 2(1), 62-86.

[8] Javeed, D., Saeed, M. S., Adil, M., Kumar, P., & Jolfaei, A. (2024). A federated learning-based zero trust intrusion detection system for Internet of Things. Ad Hoc Networks, 162, 103540.

[9] Naeem, F., Malik, A. W., Khan, S. A., & Jabeen, F. (2023, December). Enhancing Intrusion detection: Leveraging Federated Learning and Hybrid Machine Learning Algorithms on ToN_IoT Dataset. In 2023 International Conference on Frontiers of Information Technology (FIT) (pp. 73-78). IEEE.

[10] Alsaleh, S., Menai, M. E. B., & Al-Ahmadi, S. (2024). Federated Learning–Based Model to Lightweight IDSs for heterogeneous IoT Networks: State-of-the-Art, Challenges and Future Directions. IEEE Access.

[11] Benameur, R., Dahane, A., Souihi, S., & Mellouk, A. (2024, June). A Novel Federated Learning Based Intrusion Detection System for IoT Networks. In ICC 2024-IEEE International Conference on Communications (pp. 2402-2407). IEEE.

[12] Lazzarini, R., Tianfield, H., & Charissis, V. (2023). Federated learning for IoT intrusion detection. Ai, 4(3), 509-530.

[13] Rashid, M. M., Khan, S. U., Eusufzai, F., Redwan, M. A., Sabuj, S. R., & Elsharief, M. (2023). A federated learning-based approach for improving intrusion detection in industrial internet of things networks. Network, 3(1), 158-179.

[14] Attota, D. C., Mothukuri, V., Parizi, R. M., & Pouriyeh, S. (2021). An ensemble multi-view federated learning intrusion detection for IoT. IEEE Access, 9, 117734-117745.

[15] Belenguer, A., Navaridas, J., & Pascual, J. A. (2022). A review of federated learning in intrusion detection systems for IoT. arXiv preprint arXiv:2204.12443.

[16] Attique, D., Hao, W., Ping, W., Javeed, D., & Adil, M. (2024, June). EX-DFL: An Explainable Deep Federated-based Intrusion Detection System for Industrial IoT. In 2024 21st International Joint Conference on Computer Science and Software Engineering (JCSSE) (pp. 358-364). IEEE.

[17] Shukla, S., Raghuvanshi, A. S., Majumder, S., & Singh, S. (2024, March). FedHNN: A Federated Learning Based Hybrid Neural Network for Real-Time Intrusion Detection Systems. In 2024 2nd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT) (pp. 693-697). IEEE.

[18] Shen, J., Yang, W., Chu, Z., Fan, J., Niyato, D., & Lam, K. Y. (2024, June). Effective intrusion detection in heterogeneous Internet-of-Things networks via ensemble knowledge distillation-based federated learning. In ICC 2024-IEEE International Conference on Communications (pp. 2034-2039). IEEE.

[19] Mothukuri, V., Khare, P., Parizi, R. M., Pouriyeh, S., Dehghantanha, A., & Srivastava, G. (2021). Federated-learning-based anomaly detection for IoT security attacks. IEEE Internet of Things Journal, 9(4), 2545-2554.

[20] Campos, E. M., Saura, P. F., González-Vidal, A., Hernández-Ramos, J. L., Bernabé, J. B., Baldini, G., & Skarmeta, A. (2022). Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges. Computer Networks, 203, 108661.

[21] Friha, O., Ferrag, M. A., Shu, L., Maglaras, L., Choo, K. K. R., & Nafaa, M. (2022). FELIDS: Federated learning-based intrusion detection system for agricultural Internet of Things. Journal of Parallel and Distributed Computing, 165, 17-31.

[22] Popoola, S. I., Imoize, A. L., Hammoudeh, M., Adebisi, B., Jogunola, O., & Aibinu, A. M. (2023). Federated deep learning for intrusion detection in consumer-centric internet of things. IEEE Transactions on Consumer Electronics, 70(1), 1610-1622.

[23] Sarhan, M., Lo, W. W., Layeghy, S., & Portmann, M. (2022). HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection. Computers and Electrical Engineering, 103, 108379.

[24] Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Alazab, M., ... & Gadekallu, T. R. (2022). Federated learning for intrusion detection system: Concepts, challenges and future directions. Computer Communications, 195, 346-361.

[25] Abou El Houda, Z., Brik, B., & Senouci, S. M. (2022). A novel IoT-based explainable deep learning framework for intrusion detection systems. IEEE Internet of Things Magazine, 5(2), 20-23.

[26] Rashid, M. M., Khan, S. U., Eusufzai, F., Redwan, M. A., Sabuj, S. R., & Elsharief, M. (2023). A federated learning-based approach for improving intrusion detection in industrial internet of things networks. Network, 3(1), 158-179.

[27] Banabilah, S., Aloqaily, M., Alsayed, E., Malik, N., & Jararweh, Y. (2022). Federated learning review: Fundamentals, enabling technologies, and future applications. Information processing & management, 59(6), 103061.

[28] Nguyen, T. D., Marchal, S., Miettinen, M., Fereidooni, H., Asokan, N., & Sadeghi, A. R. (2019, July). DÏoT: A federated self-learning anomaly detection system for IoT. In 2019 IEEE 39th International conference on distributed computing systems (ICDCS) (pp. 756-767). IEEE.

[29] Keshk, M., Koroniotis, N., Pham, N., Moustafa, N., Turnbull, B., & Zomaya, A. Y. (2023). An explainable deep learning-enabled intrusion detection framework in IoT networks. Information Sciences, 639, 119000.

[30] Kelli, V., Argyriou, V., Lagkas, T., Fragulis, G., Grigoriou, E., & Sarigiannidis, P. (2021). IDS for industrial applications: A federated learning approach with active personalization. Sensors, 21(20), 6743.

[31] Vaiyapuri, T., Algamdi, S., John, R., Sbai, Z., Al-Helal, M., Alkhayyat, A., & Gupta, D. (2023). Metaheuristics with federated learning enabled intrusion detection system in Internet of Things environment. Expert Systems, 40(5), e13138.

[32] Singh, P., Gaba, G. S., Kaur, A., Hedabou, M., & Gurtov, A. (2022). Dew-cloud-based hierarchical federated learning for intrusion detection in IoMT. IEEE journal of biomedical and health informatics, 27(2), 722-731.

[33] Smys, S., Basar, A., & Wang, H. (2020). Hybrid intrusion detection system for internet of things (IoT). Journal of ISMAC, 2(04), 190-199.

[34] Nguyen, T. D., Rieger, P., Miettinen, M., & Sadeghi, A. R. (2020, February). Poisoning attacks on federated learning-based IoT intrusion detection system. In Proc. Workshop Decentralized IoT Syst. Secur.(DISS) (Vol. 79).

[35] Olanrewaju-George, B., & Pranggono, B. (2025). Federated learning-based intrusion detection system for the internet of things using unsupervised and supervised deep learning models. Cyber Security and Applications, 3, 100068