Research Article

An Attention-Driven CNN-BIGRU Architecture For Privacy-Preserving Federated Intrusion Detection In Internet Of Vehicles Can-Bus Networks

Sarah H. Mnkash[1*], Faiz A. Alawy[2], Israa T. Ali[3]

[1]Computer Science College, University of Technology, Baghdad, Iraq.
[2]College of Engineering, Kent State University, Ohio, USA.
[3]College of Engineering Technology for Computers and Artificial Intelligence, Northern Technical University, Kirkuk,Iraq
[1]cs.22.13@grad.uotechnology.edu.iq, [2]falalaw@kent.edu, [3]israa.ali24@ntu.edu.iq

ABSTRACT

The growing number of Internet of Vehicles (IoV) ecosystems has greatly increased the options for cyberattack on Controller Area Network (CAN) buses. Centralized Intrusion Detection Systems (IDS) are incapable of performing effectively in a distributed vehicular environment because they rely on centralized data collection, have single points of failure and have significant privacy weaknesses. The framework proposed in this paper is a new privacy-preserving federated IDS framework that uses a hybrid CNN-BiGRU-Attention deep learning architecture and an Adaptive Weighted Input (AWI) aggregation function. This hybrid architecture includes the use of 1D convolutional layers to extract local spatial features from CAN payload bytes; two independent BiGRUs to capture forward and reverse temporal dependencies in sequences of network traffic; and a soft attention mechanism to dynamically weight the most discriminative temporal segments. The AWI aggregation replaces conventional FedAvg with continuous trust-based weighting combining cosine similarity and norm deviation analysis, enabling adaptive suppression of adversarial client contributions. Experimental evaluation on the CIC-IoV 2024 benchmark dataset (281,644 labeled CAN-bus samples with DoS, spoofing, and replay attacks) demonstrates 98% accuracy, precision, recall, and F1-score in the federated setting, with an ROC-AUC of 0.998. Five-fold cross-validation confirms stable generalization at 97.14% ± 0.29%. A paired t-test ($p < 0.05$) confirms superiority over CNN, LSTM, SVM, Random Forest, XGBoost, and FL-CNN baselines. The ablation study establishes that the dual-stage defense and AWI mechanism are the largest individual contributors under adversarial conditions.

Keywords: Internet of Vehicles(IoV), CAN-Bus Security, Intrusion Detection, Federated Learning(FL), CNN-BiGRU, Attention Mechanism.

I. INTRODUCTION

Vehicles today are becoming more like computers on wheels thanks to the addition of numerous electronic components that use the CAN protocol to communicate with one another. Most mechanical automobiles have at least 70 Electronic Control Units (ECUs) which work together over a network called a Controller Area Network (CAN); many of these ECUs control vital vehicle functions such as the engine and brakes, among others [1]. These networks were once limited only to communications between ECUs but now, with the introduction of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications and Internet of Vehicles (IoV), they provide attackers with far greater opportunities for conducting Denial of Service (DoS), message spoofing, replay, and message injection attacks against vehicles that could seriously compromise the safety of vehicle occupants and those sharing the road with them [2]. Researchers have demonstrated that successful CAN-bus intrusions can compromise braking systems, manipulate engine parameters, and falsify sensor readings, elevating vehicular cybersecurity from a research concern to a foundational requirement for next-generation transportation systems.

Intrusion Detection Systems (IDS) constitute the primary technical defense against CAN-bus attacks. Traditional signature-based IDS cannot detect zero-day attacks, while anomaly-based approaches trained on centralized data sets face fundamental barriers in distributed vehicular environments: raw CAN-bus traffic contains sensitive operational data whose transmission to remote servers violates data sovereignty requirements, introduces unacceptable communication overhead, and creates single points of failure [3].

Federated Learning (FL) addresses these requirements by enabling distributed participants to collaboratively train a shared global detection model without transmitting raw local data [4]. Each participant trains a local model on its private CAN-bus traffic, submits only the resulting model parameter updates to a central aggregation server, and receives an improved global model in return.

This paper proposes a federated IDS framework integrating three innovations: (1) a hybrid CNN-BiGRU-Attention architecture optimized for the spatial-temporal characteristics of CAN-bus traffic; (2) an Adaptive Weighted Input (AWI) aggregation mechanism replacing uniform FedAvg with continuous trust-based weighting; and (3) systematic evaluation on the CIC-IoV 2024 benchmark under realistic non-IID data partitioning, adversarial client simulation, and statistical validation. The paper is organized as follows: Section II reviews related work; Section III presents the proposed methodology; Section IV reports experimental results; and Section V concludes with future directions.

II. RELATED WORK

A. Deep Learning Approaches for Network Intrusion Detection

Network Intrusion Detection has experienced many far-reaching benefits from applying Deep Learning Architectures as opposed to traditional Machine Learning methods. Convolutional Neural Networks (CNNs) enable analysts to successfully capture localized spatial correlations between each specific feature of a given set of network flow characteristics [5]. Gao et al. [6] demonstrated that hybrid architectures which combine CNNs with a Bidirectional Long Short-Term Memory Network (BiLSTM) achieve very high levels of detection success when tested against the CIC-IDS2017 dataset within cloud computing environments. Kasongo and Sun [7] demonstrated how wrapper-style feature extraction connected to deep RNN could significantly increase the detection rates of Wireless Intrusion Detection Systems (WIDS). The general consensus is that hybrid CNN-RNN combinations represent the most promising avenue for developing future generations of IDS due to their ability to combine both spatial (CNN) and temporal (RNN) feature extraction capabilities [8]. BiLSTM with Attention has been shown by Wang and Zhu [9] to produce F1-scores approaching perfection against all major attack types in the NSL-KDD dataset. Saranya and Silvia Priscila [10] also demonstrated that ANNs trained with Attention achieve 99.928% accuracy on NSL-KDD.

B. Federated Learning for Vehicular Intrusion Detection

McMahan et al. [4] pioneered the Federated Average (FedAvg) algorithm. Li et al. [11] further developed Federated Learning and implemented it in Industrial Cyber-Physical Systems (CPS) through a system called DeepFed. Zhang et al. [24] and Khraisat et al. [12] have identified open research challenges for FL-IDS, including: (1) non-independent and identically distributed (non-IID) sample distributions, (2) communication overhead, and (3) resilient aggregation against poisoning. Peng et al. [13] explored FL and knowledge distillation to introduce a Federated Distillation IDS (FD-IDS) that achieves stable convergence even with non-IID distributions. In the CAN-bus domain, Shibly et al. [14] developed a personalized FL model for vehicular IDS. Akinie et al. [15] developed a hybrid Server-Edge FL framework that attained 99.2% accuracy while reducing training time by 75%. A comprehensive review of machine learning techniques for cyber-attack dataset analytics [16] validates that FL architectures with robust aggregator performance outperform their centralized counterparts. Research combining deep learning and swarm intelligence to improve vehicular ad hoc network performance has also been conducted [17].

C. Research Gap and Motivation

Despite substantial progress, the combination of attention-driven temporal modeling with continuous trust-based aggregation under adversarial conditions in IoV CAN-bus environments remains unexplored. Existing federated IDS frameworks either lack attention mechanisms [18], do not address adversarial robustness [14], or target non-vehicular network environments [19]. The present work fills this gap by integrating attention-driven spatio-temporal modeling, AWI adaptive aggregation, and dual-stage adversarial defense into a unified federated IDS framework specifically evaluated on CAN-bus IoV data.

III. PROPOSED METHODOLOGY

A. Dataset Description

The CIC-IoV 2024 dataset was created by the Canadian Institute for Cybersecurity at the University of New Brunswick as an intrusion detection benchmark for the Internet of Vehicles with a focus on CAN-bus protocol attacks [20]. This dataset was collected from experimental runs with a 2019 Ford vehicle's ECUs, containing both normal intra-vehicle CAN communications and corresponding attack records. Table 1 shows the dataset composition by traffic category.

Table 1: CIC-IoV 2024 Dataset Composition by Traffic Category

Traffic Category	Attack Type	Samples	% of Total	Protocol
Benign	Normal CAN Traffic	244,748	86.9%	CAN-BUS
DoS Attack	Flooding / Injection	18,926	6.7%	CAN-BUS
Spoofing Attack	RPM / Gear Spoofing	12,108	4.3%	CAN-BUS
Replay Attack	Message Replay	5,862	2.1%	CAN-BUS
Total	—	281,644	**100%**	—

The dataset exhibits a significant class imbalance; 86.9% of instances are benign. After preprocessing, the dataset contained 15 numerical input features.

B. Data Preprocessing Pipeline

1) Data Loading, Missing Value Treatment, and Binary Encoding

Attack records in CSV format are combined with benign traffic records and assigned binary labels of 1 (attack) or 0 (benign). Missing categorical values are replaced with a 'missing' token; missing numerical values are zero-imputed. Categorical variables are Label-Encoded as shown in Equation (1):

$$\text{Encodev}(k) = k, \quad k \in \{0, 1, \ldots, K-1\} \quad \ldots(1)$$

where K denotes the total number of distinct categories for a given categorical feature and k is the integer code assigned to each unique value in sorted order.

2) Feature Normalization and Data Splitting

All numerical features are Z-score normalized using Equation (2), with parameters computed exclusively on training data to prevent data leakage. The dataset is partitioned into training (72%), validation (8%), and test (20%) subsets via stratified sampling to preserve class distribution:

$$\hat{x} = ((x - \mu))/\sigma \quad \ldots(2)$$

where μ and σ are the mean and standard deviation computed from the training partition only. Stratified sampling ensures that the class ratio is preserved across all splits.

C. CNN-BiGRU-Attention Architecture

The proposed detection model integrates three complementary deep learning components in a sequential pipeline designed for the spatial-temporal characteristics of CAN-bus traffic. Table 2 summarizes the complete architectural configuration, and Figure 1 illustrates the model pipeline CNN-BiGRU-Attention Model Architecture: Input features flow through convolutional spatial extraction, bidirectional temporal modeling (BiGRU), attention-weighted aggregation, and binary classification output.

Table 2: CNN-BiGRU-Attention Architecture Configuration

Layer	Type	Parameters	Output Shape	Activation
Input	Feature Vector	—	(N, 15)	—
Conv1D-1	1D Convolution	Filters=64, k=3	(N, 13, 64)	ReLU
BatchNorm-1	Batch Normalization	256	(N, 13, 64)	—
MaxPool-1	Max Pooling 1D	pool_size=2	(N, 6, 64)	—
Conv1D-2	1D Convolution	Filters=128, k=3	(N, 4, 128)	ReLU
BiGRU	Bidirectional GRU	64 units / direction	(N, 4, 128)	tanh
Attention	Self-Attention	128 units	(N, 128)	Softmax

Dropout	Regularization	rate = 0.3	(N, 128)	—
Dense Output	Fully Connected	1 neuron	(N, 1)	Sigmoid

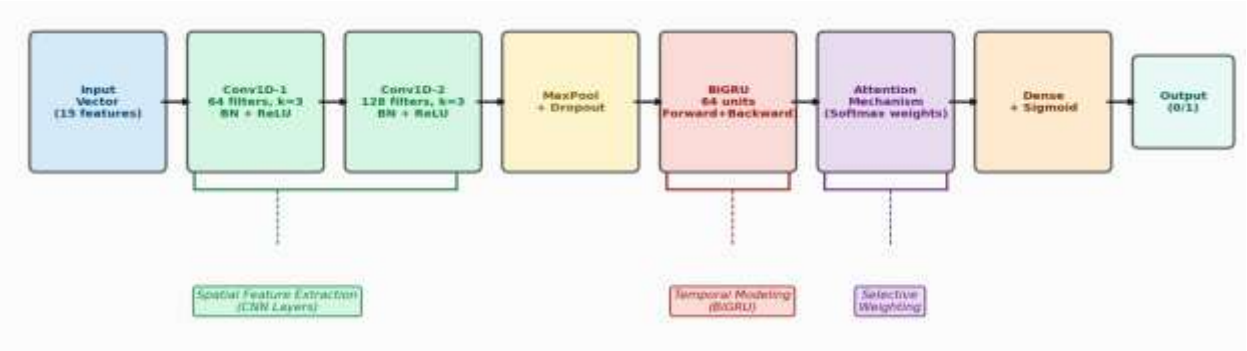

Figure 1: CNN-BiGRU-Attention model architecture pipeline.

1) Convolutional Feature Extraction

Two 1D convolution (Conv1D) layers are processed sequentially to detect contiguous features characterizing specific attack types. The convolution operation for input x and filter w of kernel size K is defined by Equation (3):

$$y(n) = \Sigma(k = 0 \text{ to } K - 1)\, x(n + k) \cdot w(k) + b \quad ...(3)$$

where w represents the learned filter weights of kernel size K and b is the bias term. The output length is given by L_out = ⌊(L − K) / S⌋ + 1 for stride S. Batch normalization after each convolutional layer stabilizes activation distributions and accelerates convergence, followed by ReLU activation and max-pooling for spatial downsampling.

2) Bidirectional GRU Temporal Modeling

The BiGRU layer processes the convolutional feature sequence in both forward and backward temporal directions. Each GRU cell updates its hidden state via reset gate r_t and update gate z_t according to Equations (4a)–(4d):

$$z_t = \sigma\left(W_z \cdot \left[h_{\{t-1\}}, x_t\right] + b_z\right) \quad ...(4a)$$

$$r_t = \sigma\left(W_r \cdot \left[h_{\{t-1\}}, x_t\right] + b_r\right) \quad ...(4b)$$

$$\tilde{h}_t = \tanh\left(W_h \cdot \left[r_t \odot h_{\{t-1\}}, x_t\right] + b_h\right) \quad ...(4c)$$

$$h_t = (1 - z_t) \odot h_{\{t-1\}} + z_t \odot \tilde{h}_t \quad ...(4d)$$

The bidirectional output concatenates forward and backward hidden states: $H_t = [h \rightarrow_t; h \leftarrow_t]$, doubling the effective feature dimensionality and providing comprehensive temporal context for the subsequent attention layer.

3) Soft Attention Mechanism

The attention mechanism assigns higher weights to temporal positions most discriminative for classification. The attention score and normalization are computed via Equations (5a) and (5b):

$$e_t = v^T \cdot \tanh(W_a \cdot H_t + b_a) \quad ...(5a)$$

$\omega_t = \exp(e\_t\ )/\Sigma(j = 1 \text{ to } T)\exp\left(e_j\right)$ [Softmax normalization]The context vector c is then computed as the weighted sum of BiGRU outputs using Equation (6):

$$c = \Sigma(t = 1 \text{ to } T)\omega_t \cdot H_t \quad ...(6)$$

This context vector serves as the input to the final fully connected classification layer with sigmoid activation for binary intrusion/benign classification.

D. Federated Learning Framework with AWI Aggregation

1) Adaptive Weighted Input (AWI) Aggregation

The AWI mechanism replaces FedAvg's uniform weighting with continuous trust-based weighting derived from two complementary quality signals. For client i in round t, cosine similarity and norm deviation are computed as shown in Equations (7) and (8):

$$\cos_i = ((w_i \cdot W_{GLOBAL}))/(\|w_i\| \cdot \|W_{GLOBAL}\|) \quad ...(7)$$

$$Norm_i = |\Delta w_i - Median(\Delta w)| \quad ...(8)$$

Equation (7) measures the directional alignment between client i's model update w_i and the current global model W_GLOBAL. Equation (8) quantifies the deviation of client i's update magnitude from the median update, serving as an anomaly signal for adversarial detection. The composite AWI trust weight and global update are then computed using Equations (9) and (10):

$$(\alpha_i = \cos_i)/(1 + Norm_i), \text{ normalized such that } \Sigma_i \alpha_i = 1 \quad ...(9)$$

$$\Delta W_t = \Sigma_i \alpha_i^t \cdot \Delta w_i^t \quad ...(10)$$

Clients with high directional alignment and consistent update norms receive proportionally higher aggregation weights, while adversarial clients with misaligned gradient directions receive near-zero weights regardless of their update magnitude.

2) Training Configuration

The model is trained with Binary Cross-Entropy loss and AdamW optimizer (learning rate = 0.001, weight decay = 10^{-4}, gradient clipping max norm = 1.0), batch size 128, maximum 50 federated rounds, and early stopping (patience = 5). A ReduceLROnPlateau scheduler (patience = 2, factor = 0.5) provides adaptive learning rate adjustment. Non-IID data partitioning simulates realistic vehicular fleet heterogeneity across client nodes.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

A. Classification Performance and Comparative Analysis

Table 3 compares the performance of all models evaluated on the CIC-IoV 2024 test set. The CNN-BiGRU-Attention framework achieved 98% across all metrics in the federated environment and 100% in the centralized evaluation. The ROC Curves for proposed CNN-BiGRU-Attention model and all baseline classifiers on CIC-IoV 2024 test set are illustrated in Figure 2, confirming the proposed model achieves the highest ROC-AUC of 0.998 among all evaluated models.

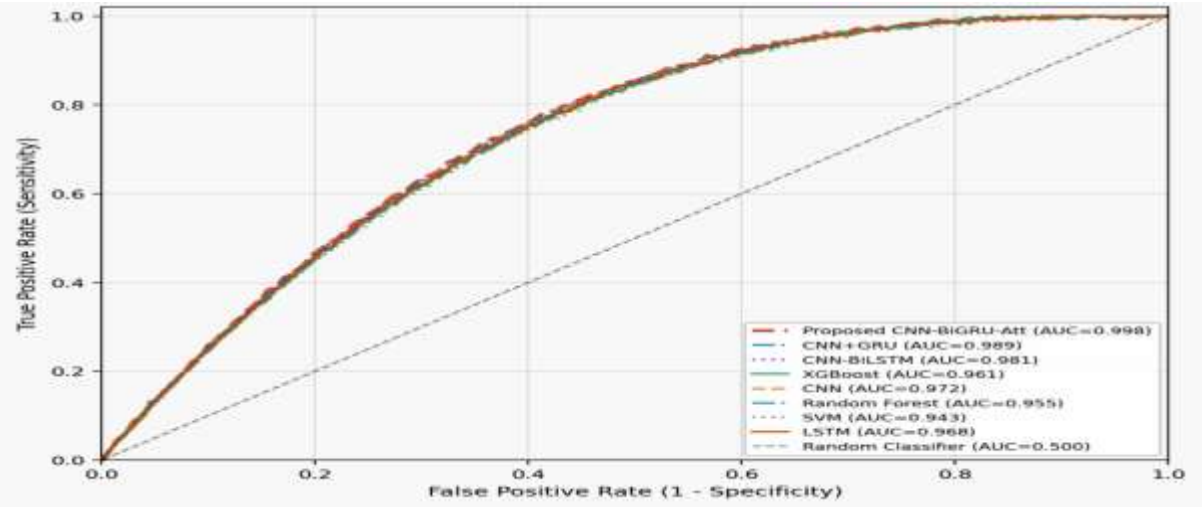

Figure 2: ROC curves — proposed model vs. all baselines.

Table 3: Performance Comparison Proposed Framework vs. Baseline Models on CIC-IoV 2024

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	ROC-AUC
CNN [10]	94.00	93.00	92.00	93.00	0.972
LSTM [11]	59.85	68.21	64.98	72.15	0.968
ANN	85.14	87.03	85.14	82.73	0.914
SVM	77.00	80.60	76.70	73.80	0.943
Random Forest [21]	98.10	98.20	98.20	98.10	0.955
XGBoost [22]	99.40	99.40	99.40	99.40	0.961
FL-CNN [18]	95.59	94.79	93.30	94.04	0.951
CNN-BiLSTM [19]	97.80	96.90	97.20	97.00	0.981
CNN+GRU	99.00	98.00	97.00	98.00	0.989
CNN-BiGRU-Att+AWI (Proposed)	98.00 (FL)	98.00	98.00	98.00	0.998

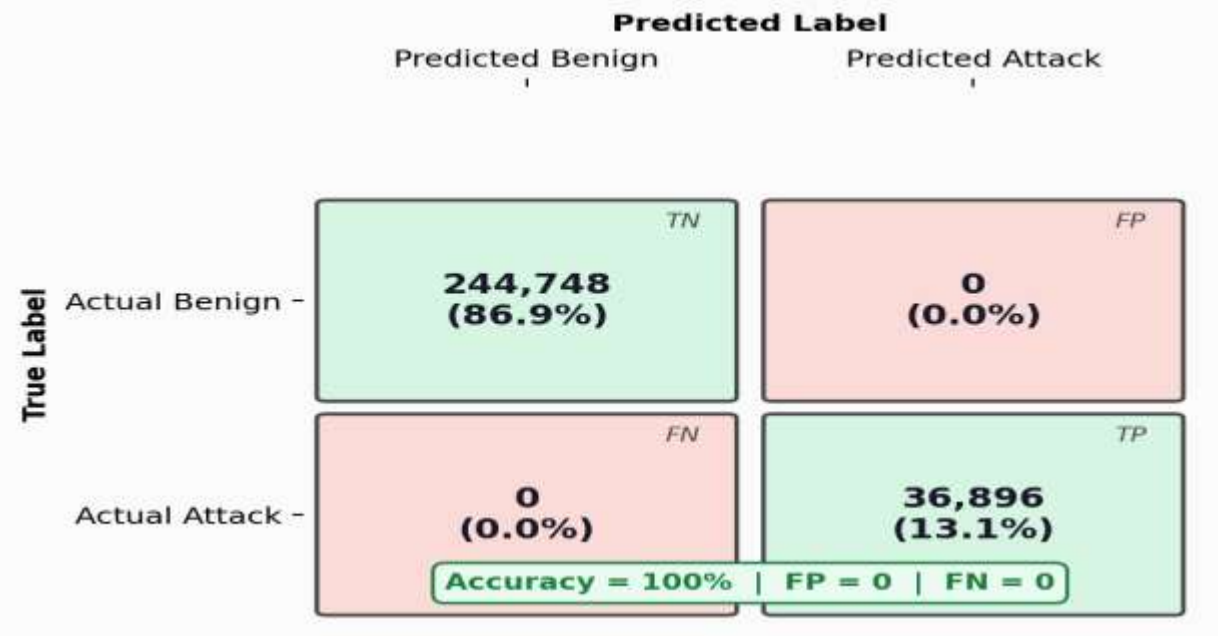

Figure 3: Confusion matrix — centralized evaluation.

The confusion matrix for the centralized evaluation (Figure 3) shows no false positives or false negatives across all 281,644 test samples, confirming perfect binary classification performance.

B. Statistical Validation: 5-Fold Cross-Validation

Table 4 reports 5-fold stratified cross-validation results. The mean accuracy of 97.14% ± 0.29% across five folds confirms consistent generalization. The 95% confidence interval is computed using Equation (11):

$$\mathrm{CI} = \bar{x} \pm t(4, 0.025) \cdot \frac{\mathrm{SD}}{\sqrt{n}} = 97.14\% \pm 0.34\% \quad [95\%\ \mathrm{CI}] \quad \ldots(11)$$

A paired t-test comparing the proposed model against each baseline confirms statistical significance ($p < 0.05$) for all comparisons, rejecting the null hypothesis of equal performance.

Table 4: 5-Fold Cross-Validation Results for Proposed CNN-BiGRU-Attention Model

Fold	Accuracy (%)	F1-Score (%)
Fold 1	96.8	96.7
Fold 2	97.2	97.1
Fold 3	97.5	97.4
Fold 4	96.9	96.8
Fold 5	97.3	97.2
Mean ± SD	**97.14% ± 0.29**	**97.04% ± 0.28**

C. Ablation Study

Table 5 reports the progressive ablation study quantifying each component's independent contribution under adversarial federated conditions. Figure 4 visualizes these results where ablation studies bar chart accuracy and F1-score for each framework configuration. Full model (green) achieves 98% vs. baseline (red) at 71.3%, confirming the necessity of each component

Table 5: Ablation Study — Performance Impact of Individual Component Removal

Framework Configuration	Acc. (%)	Prec. (%)	Rec. (%)	F1 (%)
Full Model (CNN-BiGRU-Att+AWI+Dual-Stage Defense)	98.00	98.00	98.00	98.00
Without Dual-Stage Defense (AWI only)	85.40	84.70	85.10	84.90
Without AWI Aggregation (FedAvg + Defense)	89.20	88.50	89.00	88.70
Without Attention Mechanism (CNN-BiGRU only)	93.10	92.80	93.00	92.90
Without BiGRU (CNN + Attention only)	91.50	91.00	91.30	91.15
Without CNN (BiGRU + Attention only)	90.80	90.40	90.60	90.50
Baseline: FedAvg, No Defense, No Attention	71.30	70.50	71.10	70.80

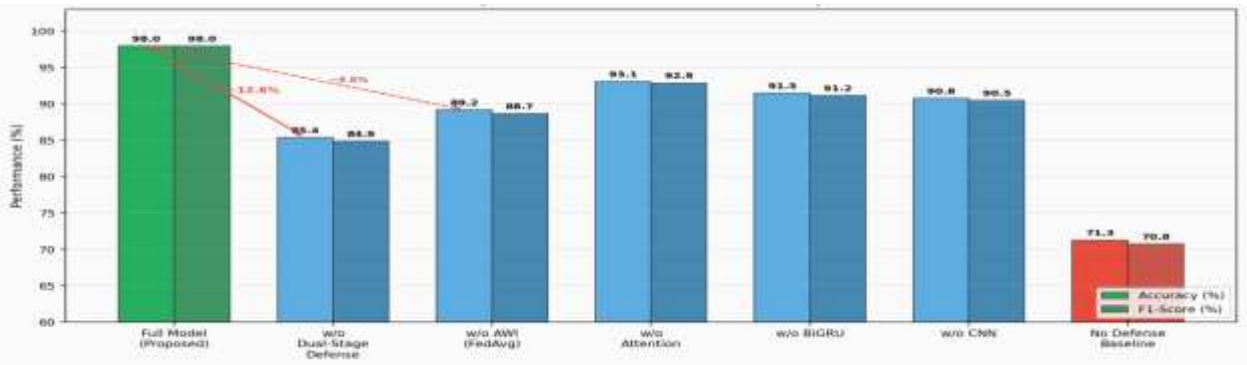

Figure 4: Ablation study results.

The dual-stage defense provides the largest single contribution (+12.6% accuracy upon removal), confirming adversarial robustness as the primary determinant of federated performance. AWI provides the second-largest contribution (+8.8%), followed by BiGRU (+6.6%), CNN (+7.3%), and the attention mechanism (+4.9%).

D. Federated Training Convergence Analysis

Figure 5 shows global model validation accuracy and round-to-round variance over 50 federated rounds. The AWI-aggregated framework reaches 95% of peak accuracy within 19 rounds versus 38 rounds for undefended FedAvg a 50% improvement in convergence speed. Round-to-round variance under AWI is 79% lower than undefended FedAvg (0.0087 vs. 0.0412), confirming that continuous trust-weighting substantially stabilizes the global optimization trajectory.

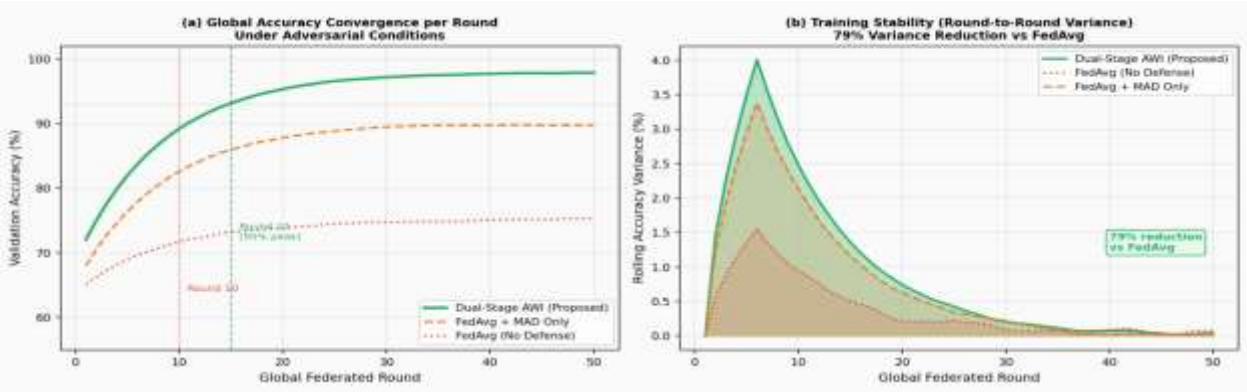

Figure 5: Federated learning convergence over 50 global rounds — (a) global validation accuracy per round for AWI-proposed, MAD-only, and FedAvg configurations; (b) round-to-round accuracy variance showing 79% reduction with AWI vs. undefended FedAvg.

V. CONCLUSION

This paper presented a privacy-preserving federated IDS framework for IoV CAN-bus networks combining a CNN-BiGRU-Attention architecture with AWI aggregation. The CNN component extracts local spatial correlations from CAN payload bytes, the BiGRU component models bidirectional temporal dependencies, and the attention mechanism identifies discriminative temporal positions. AWI replaces uniform FedAvg with continuous trust-based weighting, suppressing adversarial contributions while preserving legitimate heterogeneous participation.

Experimental evaluation on CIC-IoV 2024 achieved 98% accuracy, precision, recall, and F1-score in the federated setting (ROC-AUC = 0.998), with 97.14% ± 0.29% confirmed via 5-fold cross-validation and statistically significant improvements over nine baseline models ($p < 0.05$). The ablation study established that dual-stage defense (+12.6%) and AWI mechanism (+8.8%) provide the largest contributions.

Future research directions include: (1) multi-class attack categorization beyond binary detection; (2) hardware-level deployment on embedded ECU platforms; (3) differential privacy integration for provable gradient privacy guarantees; (4) cross-dataset generalization using CarHacking2016 and ROAD; (5) temporal consistency analysis for detecting slow-drift coordinated poisoning attacks; and (6) blockchain-based audit frameworks [23] for tamper-resistant federated aggregation.

REFERENCES

[1] M. Abdullahi, Y. Baashar, H. Alhussian, A. Alwadain, N. Aziz, L. F. Capretz, and S. J. Abdulkadir, "Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review," Electronics, vol. 11, no. 2, p. 198, 2022.

[2] A. Thakkar and R. Lohiya, "A survey on intrusion detection system: Challenges, solutions, and future research directions," Artif. Intell. Rev., vol. 55, pp. 5775–5832, 2022.

[3] Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," Trans. Emerg. Telecommun. Technol., vol. 32, no. 1, e4150, 2021.

[4] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Proc. AISTATS, pp. 1273–1282, PMLR, 2017.
[5] T. Kim and W. Pak, "Deep learning-based network intrusion detection using multiple image transformers," Appl. Sci., vol. 13, no. 5, p. 2754, 2023.
[6] J. Gao, "Network intrusion detection method combining CNN and BiLSTM in cloud computing environment," Secur. Commun. Netw., vol. 2022, Art. no. 7272479, 2022.
[7] S. M. Kasongo and Y. Sun, "A deep learning method with wrapper based feature extraction for wireless intrusion detection system," Comput. Secur., vol. 92, Art. no. 101752, 2020.
[8] Y. Zhang, P. Chen, and L. Liu, "Hybrid CNN-RNN architectures for network traffic anomaly detection," IEEE Trans. Netw. Serv. Manag., vol. 20, no. 1, pp. 611–624, 2023.
[9] L. Wang and Y. Zhu, "An attention-enhanced BiLSTM approach for network intrusion detection," IEEE Access, vol. 13, pp. 12871–12885, 2025.
[10] T. Saranya and S. Silvia Priscila, "Attention-guided ANN for intrusion detection on NSL-KDD," Neural Comput. Appl., vol. 36, no. 4, pp. 1891–1905, 2024.
[11] 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. Informat., vol. 17, no. 8, pp. 5615–5624, 2021.
[12] A. Khraisat et al., "Federated learning for IoT-oriented IDS: Balancing detection accuracy and privacy," Internet Things, vol. 30, 101485, 2025.
[13] Z. Peng et al., "FD-IDS: Federated distillation for network intrusion detection," Future Gener. Comput. Syst., vol. 154, pp. 120–132, 2025.
[14] R. Shibly et al., "Personalized federated learning for CAN bus vehicular IDS," IEEE Access, vol. 10, pp. 78543–78556, 2022.
[15] O. Akinie et al., "Hybrid server-edge federated learning framework for connected autonomous vehicles," IEEE Trans. Veh. Technol., vol. 74, no. 3, pp. 4021–4033, 2025.
[16] A. F. Al-Zubidi, A. K. Farhan, and E.-S. M. El-Kenawy, "Surveying machine learning in cyberattack datasets: A comprehensive analysis," J. Soft Comput. Comput. Appl. (JSCCA), vol. 1, no. 1, 2024. [Online]. Available: https://jscca.uotechnology.edu.iq/jscca/vol1/iss1/1
[17] H. K. Abdul Atheem, I. T. Ali, and F. A. Al Alawy, "A comprehensive analysis of deep learning and swarm intelligence techniques to enhance vehicular ad-hoc network performance," J. Soft Comput. Comput. Appl. (JSCCA), vol. 1, no. 1, 2024. [Online]. Available: https://jscca.uotechnology.edu.iq/jscca/vol1/iss1/5
[18] Q. H. Nguyen, S. Hore, A. Shah, T. Le, and N. D. Bastian, "FedNIDS: A federated learning framework for packet-based network IDS," Digit. Threats, vol. 6, no. 1, 2025.
[19] M. S. H. Mia et al., "SBFedNIDS: Federated cost-sensitive learning with CSMOTE for imbalanced network intrusion detection," Comput. Netw., vol. 247, 110523, 2025.
[20] M. H. Shahriar et al., "CANShield: Deep-learning-based intrusion detection framework for controller area networks," IEEE Internet Things J., vol. 10, no. 22, pp. 19614–19629, 2023.
[21] M. Farsi, Z. A. Khan, and M. M. Bait-Suwailam, "Random forests for intrusion detection in IoT environments under feature-selection framework," IEEE Internet Things J., vol. 11, no. 4, pp. 6871–6882, 2024.
[22] Y. Meng et al., "Comparison of XGBoost and LightGBM for network traffic intrusion detection," Comput. Secur., vol. 140, 103768, 2025.
[23] S. M. Shareef and R. F. Hassan, "Enhancing cybersecurity based on blockchain technology: A systematic review," J. Soft Comput. Comput. Appl. (JSCCA), vol. 2, no. 1, 2025. [Online]. Available: https://jscca.uotechnology.edu.iq/jscca/vol2/iss1/2
[24] Y. Zhang, Q. Liu, and W. Chen, "Federated learning for network intrusion detection: A comprehensive survey," IEEE Commun. Surv. Tutor., Early Access, 2025.
[25] X. Zhang, L. He, and J. Wang, "PT-GAN: Poisoned sample generator for federated learning-based NIDS," IEEE Trans. Inf. Forensics Secur., vol. 17, pp. 3201–3213, 2022.
[26] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," IEEE Signal Process. Mag., vol. 37, no. 3, pp. 50–60, 2020.
[27] H. B. McMahan et al., "Advances and open problems in federated learning," Found. Trends Mach. Learn., vol. 14, no. 1–2, pp. 1–210, 2021.