Fuse and Federate: Enhancing EV Charging Station Security with Multimodal Fusion and Federated Learning

Rabah Rahal[1], Abdelaziz Amara korba[1,2], and Yacine Ghamri-Doudane[2]

[1]*Networks and Systems Laboratory (LRS), Badji Mokhtar Annaba University, Algeria*
[2]*L3I, University of La Rochelle, France*

***Abstract*—The rapid global adoption of electric vehicles (EVs) has established electric vehicle supply equipment (EVSE) as a critical component of smart grid infrastructure. While essential for ensuring reliable energy delivery and accessibility, EVSE systems face significant cybersecurity challenges, including network reconnaissance, backdoor intrusions, and distributed denial-of-service (DDoS) attacks. These emerging threats, driven by the interconnected and autonomous nature of EVSE, require innovative and adaptive security mechanisms that go beyond traditional intrusion detection systems (IDS). Existing approaches, whether network-based or host-based, often fail to detect sophisticated and targeted attacks specifically crafted to exploit new vulnerabilities in EVSE infrastructure. This paper proposes a novel intrusion detection framework that leverages multimodal data sources, including network traffic and kernel events, to identify complex attack patterns. The framework employs a distributed learning approach, enabling collaborative intelligence across EVSE stations while preserving data privacy through federated learning. Experimental results demonstrate that the proposed framework outperforms existing solutions, achieving a detection rate above 98% and a precision rate exceeding 97% in decentralized environments. This solution addresses the evolving challenges of EVSE security, offering a scalable and privacy-preserving response to advanced cyber threats.**

***Index Terms*—Electric Vehicle Supply Equipment (EVSE), Intrusion Detection System (IDS), Federated Learning, Cybersecurity, Multimodal Data Fusion**

I. Introduction

The global electric vehicle (EV) market has surged from 26 million EVs on the road in 2022 to over 40 million in 2024, reflecting a 53.85% growth rate in sales [1]. This rapid expansion makes it imperative to adapt current smart grid infrastructure, including Electric Vehicle Supply Equipment (EVSE), to meet the demands of this fast-growing sector. Each EVSE deployed must provide flexible payment solutions for access to services, such as credit card payments, mobile applications, or prepaid monthly cards. However, this accessibility to sensitive payment and user information has made EVSEs an attractive target for cyber threats, emphasizing the need for robust cybersecurity measures to protect user confidentiality and privacy.

Despite advances in securing traditional infrastructure, EVSEs continue to exhibit significant vulnerabilities. Recent incidents underscore the associated risks: in 2024, ransomware attacks on charging stations surged by 90%, with cybercriminals encrypting station systems and demanding ransom payments for restoration [2]. Furthermore, research has identified critical flaws in the widely-used Open Charge Point Protocol (OCPP), making charging sessions vulnerable to disruptions and unauthorized data access [3], [4]. These incidents emphasize the urgent need for advanced cybersecurity solutions to protect EVSEs from a wide array of threats. Current security mechanisms, such as network-based [4], [5] and host-based IDS, often rely on modeling the behavior of EV charging stations using a single type of log within their local scope. This approach may lack the depth and adaptability required to detect sophisticated attack patterns and multi-layered cyber threats targeting EVSEs.

Current intrusion detection systems (IDS) for EV charging infrastructure have made progress in addressing cyber threats but face significant limitations. Many rely on complex architectures or multiple sub-models, which can be resource-intensive and unsuitable for deployment on constrained EVSEs [6], [7]. Others focus on specific attack scenarios like injection attacks in vehicle-to-grid communication but lack flexibility for diverse threats [8], [9]. Emerging AI-driven solutions incorporating blockchain and reinforcement learning (RL) show promise - blockchain ensures transaction security [10], [11] despite interoperability and storage challenges, while RL enables dynamic adaptation [12], [13] though requiring extensive data and raising ethical concerns. However, these advanced approaches still struggle with high computational costs, poor cross-network generalization, and the fundamental trade-off between scalability, adaptability, and resource efficiency. This highlights the critical need for more robust IDS frameworks capable of leveraging diverse data sources while overcoming these persistent limitations.

Developing a robust IDS for EVSEs is crucial to address cyberattacks like vulnerability scanning, network intrusions, and host-targeted attacks. Existing IDS solutions often focus on a single data source, such as network traffic [14]–[17] or kernel logs [18], offering limited threat insight. Network traffic lacks host-level visibility, while kernel logs miss external attack patterns. Centralizing EVSE logs for global IDS training raises significant privacy concerns.

To address these challenges, our framework employs a comprehensive approach by intelligently processing and fusing diverse log types generated by EVSEs during operation. This

enables the IDS to correlate information across multiple data sources, uncovering complex attack patterns that cannot be detected by analyzing a single log type alone.

- **Multimodal Data Fusion**: Our approach utilizes diverse data types generated by EVSEs, including network traffic and kernel events, to construct a comprehensive view of station activity. While this paper focuses on these two data sources, the framework's design, leveraging latent representation extraction and compression, is inherently extensible to incorporate other types of data logs, such as power consumption and voltage metrics.
- **Privacy-Preserving Collaboration**: Through Federated Learning (FL), the framework capitalizes on the diversity of logs collected by a large number of geographically distributed EVSEs, enabling collaborative model training without compromising data privacy.
- **Decentralized Security**: This decentralized approach ensures high detection accuracy while preserving the confidentiality of user and operational data.

By combining multimodal data fusion and federated learning, the framework significantly improves the detection of sophisticated attack patterns, providing a robust, scalable, and privacy-preserving cybersecurity solution for EVSE infrastructure.

The remainder of this paper is organized as follows: Section 2 reviews background and literature review; Section 3 defines the problem and model framework; Section 4 introduces the proposed methodology; Section 5 presents experiments and results; and Section 6 concludes with future research directions.

II. Background and Related Work

This section reviews EVSE foundations, focusing on key features, protocols, attack scenarios, and recent intrusion detection research.

A. EVSE Characteristics and Communication Protocols

The Electric Vehicle Supply Equipment (EVSE) ecosystem depends on key communication protocols for interoperability, security, and efficiency. Two main protocols are central to this: the Open Charge Point Protocol (OCPP) and ISO 15118.

OCPP, developed by the Open Charge Alliance, is a widely adopted protocol for managing communication between EV chargers and central systems. It facilitates features such as smart charging, remote diagnostics, and enhanced security, ensuring compatibility and centralized control across diverse EVSE networks [19]. On the other hand, ISO 15118, an international standard for EVs, governs communication between vehicles and charging stations. This protocol introduces Plug & Charge functionality, allowing automatic vehicle authentication, which improves user convenience and security. Additionally, ISO 15118 supports bidirectional energy transfer, enabling advanced vehicle-to-grid (V2G) services that enhance grid stability and energy efficiency [20].

B. Related Work

In [6], the authors proposed an IDS using ensemble learning for EVSE networks, targeting attack detection in both centralized and decentralized infrastructures. Their framework combines multiple models trained on diverse EVSE data to improve detection accuracy. However, relying on three classification sub-models may not suit all EVSEs, particularly those with limited computational resources.

Researchers in [7] proposed an IDS for IoT-based EV charging stations to detect cyber threats, using a real IoT dataset with both binary and multiclass classification. They apply PCA for feature selection and evaluate performance with a CNN-A-LSTM model. However, the complex CNN-A-LSTM architecture poses risks of overfitting, highlighting potential limitations in generalization.

In [8], the authors present an injection attack on vehicle-to-grid (V2G) communication at public EV charging stations, exploiting ISO 15118 protocol flaws. Their custom testbed simulates malicious packet injections between the EV communication controller (EVCC) and the station's Supply Equipment Communication Controller (SECC), leading to denial-of-service, remote code execution, and malware spread. They propose a machine learning-based IDS trained on benign and malicious traffic. However, the 64KB message size limit may reduce realism and hinder detection of complex threats, affecting IDS effectiveness.

Poudel et al. [9] analyzed malware propagation in V2G communications at EVSEs, demonstrating malicious traffic injection risks. Their model maps EVSE connectivity to calculate malware spread probabilities, optimizing attacks for high-risk locations. Tests in urban/rural areas show optimal strategies increase spread by 10–33%, revealing critical power-transportation vulnerabilities.

Several studies [21]–[23] have developed anomaly detection systems to monitor EV charging behavior. While innovative, these approaches have some key blind spots. For example, [21]'s clustering method identifies typical charging profiles well, but because it relies solely on historical data, it fails to detect sophisticated attacks where hackers mimic normal charging patterns. Behavior-based detection also faces challenges – without massive, diverse datasets, these systems often struggle to distinguish true threats from natural variations in EVSE usage.

Even though EVSE security has been enhanced by contemporary IDS solutions, edge deployment may not be feasible due to their weight. Our approach addresses this by combining host and network data in a smart and efficient way. Federated learning allows chargers to collaborate to improve detection while ensuring that training remains local (no data sharing is required), which is perfect for real-world EVSEs with constrained resources and ever-evolving threats.

III. Proposed Solution

A. Overview

We propose an intrusion detection framework for EVSE stations that leverages multiple log types, including network

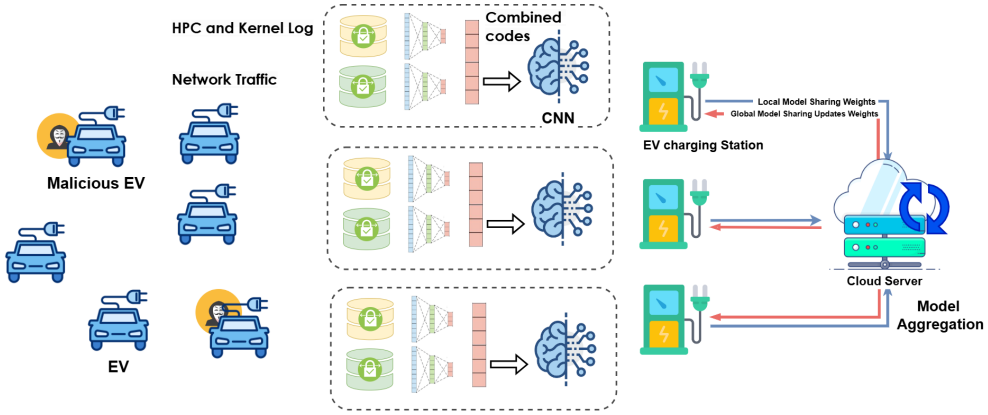

Fig. 1: Federated Training of the Intrusion Detection Model

traffic and kernel events, to detect potential attacks. Operating locally on each EVSE as a host-based, multimodal system, the IDS uses feature extraction and an autoencoder to create compressed embeddings, which are fused to manage data dimensionality. This multimodal data fusion is integrated into federated training, where a cloud server acts as a parameter server and edge servers at charging stations function as clients, collaboratively training the detection model. By analyzing threats from multiple perspectives. Importantly, the overall framework is designed to be lightweight. It relies on a single CNN model and compact latent representations, which significantly reduces inference-time computation. In contrast to late fusion multimodal approaches that require multiple parallel models, our method is more energy-efficient and better suited for resource-constrained edge environments. Figure 1 illustrates the federated learning framework, with subsequent sections detailing the system architecture and training process.

B. Feature Encoding and Fusion with Autoencoders

Our system relies on two key types of data logs, each offering insights from a different perspective. The first, Network Traffic Logs (D_1), captures real-time communications between the charging station and external entities, such as payment gateways and central servers. Anomalies in network traffic, such as unusual spikes or abnormal request patterns, can indicate potential attacks. The second, Kernel Event Logs and High Performance Counter (HPC) Metrics (D_2), includes low-level kernel event logs and hardware performance metrics, providing a system-level view of charging station operations. These records are essential for detecting covert activities, such as privilege escalations or backdoor installations. For each dataset, relevant features are extracted based on statistical and domain-specific criteria, resulting in a feature vector $x_i^{(j)}$ for each dataset D_j, where i denotes the station. Formally, the transformation can be represented as:

$$x_i^{(j)} = f_j(\text{preprocess}(D_j)), \tag{1}$$

where f_j is the specific feature extraction function applied to each dataset.

We apply a dedicated autoencoder to each dataset to learn meaningful patterns in a compact latent space. The encoder-decoder structure compresses the input while preserving essential features. For each feature vector $x_i^{(j)}$ extracted from dataset D_j, we apply an autoencoder g_j to obtain a latent representation $z_i^{(j)}$:

$$z_i^{(j)} = g_j(x_i^{(j)}), \quad j \in \{1, 2\}, \tag{2}$$

where g_j denotes the encoding function for each dataset D_j, preserving each modality's unique features in a compressed form for efficient storage and processing.

We adopt intermediate fusion by combining latent representations $z_i^{(1)}$ and $z_i^{(2)}$ from different data sources into a unified vector z_i, capturing the station's overall state. Unlike early fusion, which merges raw inputs and may lack semantic depth, this approach integrates multimodal insights to enhance prediction quality. The combined vector z_i is defined as:

$$z_i = f_{\text{concat}}(z_i^{(1)}, z_i^{(2)}), \tag{3}$$

where f_{concat} is the concatenation function, merging network and system features into a shared latent space.

C. Attacks Detection

For intrusion detection on fused vector z_i, we employ a 1D CNN, effective at capturing sequential/spatial patterns in latent features to identify malicious anomalies.

The CNN processes z_i through multiple layers, each with distinct functions. The initial layers of the CNN apply convolutions to z_i, extracting critical feature patterns. For a convolutional filter k of size M, the convolution operation on z_i produces an output $c_i^{(k)}$ as follows:

$$c_i^{(k)} = \sigma\left(\sum_{m=1}^{M} w_m^{(k)} z_{i,m} + b^{(k)}\right), \tag{4}$$

where $w^{(k)}$ and $b^{(k)}$ are the filter's weights and biases, and σ is a non-linear activation function, such as ReLU.

Convolutional outputs pass through pooling layers to reduce dimensionality and capture key features:

$$p_i^{(k)} = \max(c_i^{(k)}), \tag{5}$$

where $p_i(k)$ represents the max-pooled value for filter k, Emphasizing prominent features while preserving spatial information, a softmax function outputs the intrusion probability:

$$\hat{y}_i = \text{softmax}(W \cdot p_i + b), \tag{6}$$

where W and b are the weights and bias of the final classification layer.

Algorithm 1: FED MDF-Based Attack Detection

Input: Multimodal datasets $\{D_1, D_2, \ldots, D_M\}$ for each station i, with N stations
Output: Intrusion detection probabilities $\{\hat{y}_i\}$ for each station i

for *each station* $i = 1$ *to* N **do**
  for $j = 1$ *to* M **do**
    $x_i^{(j)} \leftarrow f_j(\text{preprocess}(D_j))$; `// Extract features from` D_j
  end for
  for $j = 1$ *to* M **do**
    $z_i^{(j)} \leftarrow g_j(x_i^{(j)})$; `// Encode features into latent space`
  end for
  $z_i \leftarrow f_{\text{concat}}(z_i^{(1)}, z_i^{(2)}, \ldots, z_i^{(M)})$; `// Combine latent vectors`
  Initialize: CNN parameters θ_i for station i;
  $p_i \leftarrow \text{CNN}_{\text{1D}}(z_i; \theta_i)$; `// Process with 1-D CNN to extract intrusion features`
  $\hat{y}_i \leftarrow \text{softmax}(W \cdot p_i + b)$; `// Calculate intrusion probability`
  Compute gradients: $\nabla_{\theta_i} \mathcal{L}(h(z_i; \theta_i), y_i)$;
end for
Federated Aggregation: Update global CNN parameters;
$\theta_{t+1} \leftarrow \theta_t - \eta \sum_{i=1}^{N} \nabla_{\theta_i} \mathcal{L}(h(z_i; \theta_t), y_i)$;
return Intrusion probabilities $\{\hat{y}_i\}$ for each station i;

To maintain data privacy, the CNN is trained using federated learning. Each charging station trains its local model on the fused vector z_i, updating the model parameters locally. Only the gradients or parameter updates are shared with a central server, which aggregates these updates to improve the global model without accessing raw data. The global parameter update is formulated as:

$$\theta_{t+1} = \theta_t - \eta \sum_{i=1}^{N} \nabla_\theta \mathcal{L}(h(z_i; \theta_t), y_i), \tag{7}$$

where: θ_t represents the CNN parameters at iteration t, η is the learning rate, and $\mathcal{L}$ is the local loss function, such as cross-entropy, computed at each station i.

The federated approach enables distributed training while preserving privacy and maintaining CNN detection effectiveness across stations. Algorithm 1 outlines the smart contract's on-chain aggregation.

IV. Experiments and Results

This section outlines the experimental setup and testing scenarios for evaluating separate/fused models and centralized/federated approaches in our framework.

A. Datasets

In this research, we used CICEVSE2024 [24], which is one of the newest publicly available datasets containing both benign and malicious traffic generated from a realistic testbed for Electric Vehicle Supply Equipment (EVSE). It includes data from three sources: Power consumption, Network Traffic, and HPC/Kernel Events (Table I). The testbed involved an operational Level 2 charging station (EVSE-A), Raspberry Pi devices for various system components (EVCC, EVSE-B, Power Monitor, Charging Station Management System (CSMS)), and communication via OCPP and ISO15118 protocols. Malicious data was generated through both network-based (e.g., DoS and TCP port scanning) and host-based attack scenarios. The three datasets are available in CSV format with extracted features.

TABLE I: Dataset samples distribution

	Network	**HPC/Kernel**
Benign	2000	32303
DoS	65790	65790
Recon	65790	65790

B. Experimental Results

The system was trained and tested in Google Colab using PyTorch for local and federated models. An autoencoder condensed the data into 32 key features via its bottleneck layer. For classification, we used a 1D CNN with two convolutional layers (each followed by max-pooling) and a dense layer. Training employed the Adam optimizer, categorical crossentropy loss, and accuracy metrics. Key CNN hyperparameters are in Table II.

To evaluate detection performance, we measured the false positive rate (FPR) alongside key metrics: accuracy, precision, recall, and F1-score.

1) Separate vs. Fused Models: We evaluated detection performance by comparing single-modal models, focused on network traffic and kernel data, with our multimodal approach, which fuses both data sources. A local comparative experiment (excluding Federated Learning) was conducted to assess the impact of data fusion on performance. The results, presented in Figure 2, show that the fusion-based model achieves superior detection performance with an accuracy of 92.91%, compared to 92.21% for the network-based model and 90.54% for the kernel-based model. Additionally, the fusion approach outperforms single-modal models across other metrics, including Precision and F1-Score. The improvement in performance,

highlights the effectiveness of using a single, unified model that outperforms models trained on separate data sources.

TABLE II: CNN Model Configuration and Hyperparameters

Parameter	Description
Model Type	1D Convolutional Neural Network (CNN)
Loss Function	categorical_crossentropy
Evaluation Metric	accuracy
Optimizer	adam
Epochs	10
Batch Size	32
Aggregation	Weighted Average

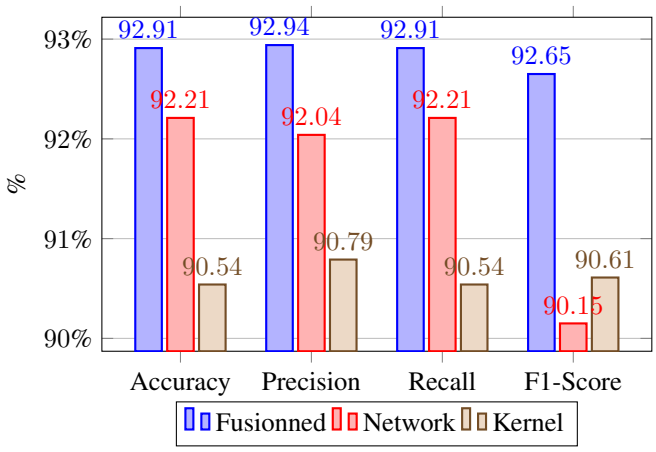

Fig. 2: Comparison of performance metrics for Fusionned, Network, and Kernel models.

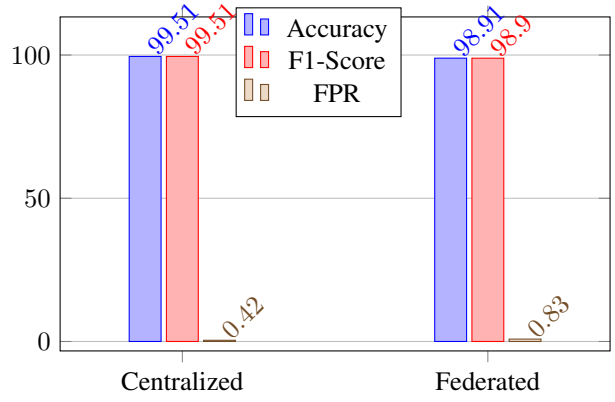

Fig. 3: Performances comparison between centralized and federated learning

2) Centralized vs. federated: We compare the results for both the centralized and federated models across 10 Charging Station (CS). The results are shown in Table III and Fig. 3.

The centralized model achieves near-perfect performance across all clients, with metrics often exceeding 99%. For instance, Client 3 recorded 100% in accuracy, precision, recall, and F1 scores, highlighting its ability to generalize effectively by leveraging a comprehensive, centralized dataset. The federated model shows a slight performance drop, with accuracy ranging from 98% to 99%, such as 98.36% for Client 9. Despite this, it maintains strong detection rates while preserving data privacy, striking a practical balance between accuracy and decentralization.

C. Federated Performance Across Client Numbers

The results in Table IV illustrate that the federated learning model maintains robust performance even as the number of clients increases. With 10 clients, the model achieves an impressive accuracy of 98.91% and an F1-score of 98.90%, with a low false positive rate (FPR) of 0.83%. This consistency across metrics, regardless of client count, underscores the model's capacity to handle distributed data effectively without compromising accuracy. While the FPR sees a slight uptick with more clients, the model continues to deliver reliable results, affirming its scalability and adaptability across diverse data sources while retaining high accuracy and minimal false positives.

1) Discussion: The results show that, although the centralized model slightly outperforms the federated approach for some clients, the federated framework still achieves performance levels close to those of the centralized model. The small performance differences can be attributed to local variations in data distribution, which tend to be more pronounced in federated settings. Nonetheless, the federated model proves to be an effective and practical solution, striking a balance between privacy and detection accuracy across a distributed system. These findings highlight the potential of federated learning to maintain high accuracy while ensuring that individual EVSEs retain control over their own data.

V. Conclusion and Future Work

We propose a federated multimodal IDS for Electric Vehicle Supply Equipment (EVSE). Our findings highlight the effectiveness of combining data fusion with federated learning, enhancing intrusion detection across EVSE networks. By integrating multiple data sources, our framework enables comprehensive threat detection with high accuracy. The federated approach keeps data decentralized, ensuring privacy without compromising performance. This combination provides a scalable, secure solution for EVSE infrastructure in the smart grid ecosystem. Future work will optimize model efficiency, integrate additional data modalities, and explore real-time deployment in more EVSE scenarios. We will also address FL robustness against poisoning attacks through secure aggregation techniques.

Acknowledgment

This work is supported by the OPEVA project that has received funding within the Chips Joint Undertaking (Chips JU) from the European Union's Horizon Europe Programme and the National Authorities (France, Czechia, Italy, Portugal, Turkey, Switzerland), under grant agreement 101097267. In France, the project is funded by BPI France under the France

TABLE III: Experimental Results

	CS 1	CS 2	CS 3	CS 4	CS 5	CS 6	CS 7	CS 8	CS 9	CS 10
Centralized	**Acc: 99.38**	**Acc: 99.79**	**Acc: 100.00**	**Acc: 99.59**	**Acc: 98.77**	**Acc: 99.59**	**Acc: 99.79**	**Acc: 99.38**	**Acc: 99.18**	**Acc: 99.59**
	Pre: 99.40	Pre: 99.80	Pre: 100.00	Pre: 99.62	Pre: 98.76	Pre: 99.59	Pre: 99.80	Pre: 99.39	Pre: 99.21	Pre: 99.60
	Rec: 99.38	Rec: 99.79	Rec: 100.00	Rec: 99.59	Rec: 98.77	Rec: 99.59	Rec: 99.79	Rec: 99.38	Rec: 99.18	Rec: 99.59
	F1: 99.39	F1: 99.80	F1: 100.00	F1: 99.60	F1: 98.75	F1: 99.59	F1: 99.80	F1: 99.38	F1: 99.18	F1: 99.59
Federated	**Acc: 98.97**	**Acc: 98.77**	**Acc: 98.97**	**Acc: 98.36**	**Acc: 98.97**	**Acc: 98.97**	**Acc: 98.77**	**Acc: 98.97**	**Acc: 98.77**	**Acc: 98.97**
	Pre: 98.98	Pre: 98.80	Pre: 99.00	Pre: 98.38	Pre: 98.97	Pre: 98.98	Pre: 98.87	Pre: 98.98	Pre: 98.88	Pre: 98.98
	Rec: 98.97	Rec: 98.97	Rec: 98.98	Rec: 98.36	Rec: 98.97	Rec: 98.97	Rec: 98.87	Rec: 98.97	Rec: 98.77	Rec: 98.97
	F1: 98.97	F1: 98.97	F1: 99.00	F1: 98.37	F1: 98.96	F1: 98.97	F1: 98.76	F1: 98.97	F1: 98.87	F1: 98.97

TABLE IV: Performance Metrics by Number of Clients

Nb. CS	Accuracy (%)	F1-Score (%)	False Positive Rate ((%)
10	98.91	98.90	0.83
8	98.64	98.63	1.52
6	98.89	98.88	0.67
3	99.61	99.61	0.40

2030 program on "Embedded AI". Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Chips JU. Neither the European Union nor the granting authority can be held responsible for them.

REFERENCES

[1] H. Ritchie and M. Roser, "Tracking global data on electric vehicles," March 12 2024, accessed: 28/10/2024. [Online]. Available: https://ourworldindata.org/electric-car-sales

[2] CNEWS, "Voitures électriques : pourquoi les bornes de recharge sont-elles de plus en plus ciblées par les hackers ?" *CNEWS*, 2024. [Online]. Available: https://www.cnews.fr/france/2024-10-28/voitures-electriques-pourquoi-les-bornes-de-recharge-sont-elles-de-plus-en-plus

[3] Numerama, "Les véhicules électriques sont une nouvelle mine d'or pour les hackers," *Numerama*, 2023. [Online]. Available: https://www.numerama.com/cyberguerre/1294758-les-vehicules-electriques-sont-une-nouvelle-mine-dor-pour-les-hackers.html

[4] A. Diaf, A. A. Korba, N. E. Karabadji, and Y. Ghamri-Doudane, "Beyond detection: Leveraging large language models for cyber attack prediction in iot networks," in *2024 20th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*. IEEE, 2024, pp. 117–123.

[5] A. A. Korba, S. Sebaa, M. Mabrouki, Y. Ghamri-Doudane, and K. Benatchba, "A life-long learning intrusion detection system for 6g-enabled iov," in *2024 International Wireless Communications and Mobile Computing (IWCMC)*, 2024, pp. 1773–1778.

[6] S. R. Hegde, V. V. Chandrakala, G. K. T., and V. K. A. Shankar, "Enhancing anomaly detection in electric vehicle supply equipment (evse) networks using classical and ensemble learning approaches," in *2024 Control Instrumentation System Conference (CISCON)*, 2024, pp. 1–5.

[7] G. Balakrishna, A. Kumar, T. V., A. Younas, N. M. G. Kumar, and R. Rastogi, "A novel ensembling of cnn-a-lstm for iot electric vehicle charging stations based on intrusion detection system," in *2023 International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS)*, 2023, pp. 1312–1317.

[8] S. Poudel, J. E. Baugh, A. Takiddin, M. Ismail, and S. S. Refaat, "Injection attacks and detection strategy in front-end vehicle-to-grid communication," in *2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2023, pp. 1–6.

[9] S. Poudel, M. Abouyoussef, J. E. Baugh, and M. Ismail, "Attack design for maximum malware spread through evs commute and charge in power-transportation systems," *IEEE Systems Journal*, vol. 18, no. 3, pp. 1809–1820, September 2024.

[10] A. Chowdhury, S. S. Shafin, S. Masum, J. Kamruzzaman, and D. Shi, "Secure electric vehicle charging infrastructure in smart cities: A blockchain-based smart contract approach," *Smart Cities*, vol. 8, no. 1, p. 33, 2025.

[11] M. S. Hossain, C. Rodine, and E. E. Tsiropoulou, "A blockchain and pki-based secure vehicle-to-vehicle energy-trading protocol," *Energies*, vol. 17, no. 17, p. 4245, 2024.

[12] M. Basnet and M. H. Ali, "Deep reinforcement learning-driven mitigation of adverse effects of cyber-attacks on electric vehicle charging station," *Energies*, vol. 16, no. 21, p. 7296, 2023.

[13] M. A. Alomrani, M. H. K. Tushar, and D. Kundur, "Detecting state of charge false reporting attacks via reinforcement learning approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 10, pp. 10 467–10 476, 2023.

[14] A. A. Korba, A. Diaf, and Y. Ghamri-Doudane, "Ai-driven fast and early detection of iot botnet threats: A comprehensive network traffic analysis approach," in *2024 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE, 2024, pp. 1779–1784.

[15] A. A. Korba, A. Boualouache, B. Brik, R. Rahal, Y. Ghamri-Doudane, and S. M. Senouci, "Federated learning for zero-day attack detection in 5g and beyond v2x networks," in *ICC 2023-IEEE International Conference on Communications*. IEEE, 2023, pp. 1137–1142.

[16] A. Tellache, A. Mokhtari, A. A. Korba, and Y. Ghamri-Doudane, "Multi-agent reinforcement learning-based network intrusion detection system," in *NOMS 2024-2024 IEEE Network Operations and Management Symposium*. IEEE, 2024, pp. 1–9.

[17] A. A. Korba, A. Boualouache, and Y. Ghamri-Doudane, "Zero-x: A blockchain-enabled open-set federated learning framework for zero-day attack detection in iov," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 9, pp. 12 399–12 414, 2024.

[18] H. Satilmiş, S. Akleylek, and Z. Y. Tok, "A systematic literature review on host-based intrusion detection systems," *IEEE Access*, vol. 12, pp. 27 237–27 266, 2024.

[19] N. F. Kamal, A. Sharida, S. Bayhan, H. Alnuweiri, and H. Abu-Rub, "Private metering in ev charging infrastructure: An ocpp extension," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 10, pp. 15 456–15 466, October 2024.

[20] A. Kilic, "Tls-handshake for plug and charge in vehicular communications," *Computer Networks*, vol. 243, p. 110281, 2024.

[21] M. Forte, C. P. Guzman, A. Lekidis, and H. Morais, "Clustering methodologies for flexibility characterization of electric vehicles supply equipment," *Green Energy and Intelligent Transportation*, p. 100304, 2025.

[22] A. Almadhor, S. Alsubai, I. Bouazzi, V. Karovic, M. Davidekova, A. Al Hejaili, and G. A. Sampedro, "Transfer learning for securing electric vehicle charging infrastructure from cyber-physical attacks," *Scientific Reports*, vol. 15, no. 1, p. 9331, 2025.

[23] S. Shirvani and A. Ghorbani, "A study of ev-evse ecosystem integrity: Machine learning based security monitoring of charging sessions," *Available at SSRN 4711137*, 2024.

[24] E. D. Buedi, A. A. Ghorbani, S. Dadkhah, and R. L. Ferreira, "Enhancing ev charging station security using a multi-dimensional dataset: Cicevse2024," in *Data and Applications Security and Privacy XXXVIII, DBSec 2024, Lecture Notes in Computer Science*, A. L. Ferrara and R. Krishnan, Eds. Springer, Cham, 2024, vol. 14901, pp. 1–15.