Scalable Hybrid Online ML for Real-Time EVCS Intrusion Detection

[1]*Hamsa C K,* [2]*Kavanashree H R,* [3]*Keerthana S S,* [4] *Manasa R,* [5] *Mr. Mohammed Kaleem*
[1234]*Don Bosco Institute of Technology Visvesvaraya Technological University, Bengaluru, India.*
[5]*Assistant Professor, Computer Science and Engineering, Don Bosco Institute of Technology, Bengaluru, India.*

Abstract : Electric Vehicle Charging Stations (EVCS) rely on networked communication protocols (such as OCPP, ISO 15118, and OCPI), exposing infrastructure to cyber threats like DoS, spoofing, and unauthorized access. This paper presents a scalable, real-time multi-class Intrusion Detection System (IDS) designed for EVCS environments. Using the UNSW-NB15 benchmark dataset, the system performs missing value imputation, categorical encoding, and standard scaling. Multi-class classification is implemented using a Histogrambased Gradient Boosting Classifier (HistGradientBoostingClassifier). An interactive dashboard served via a Python HTTP microserver provides live threat analysis, attack classification, and automated prevention recommendations. Experimental results demonstrate strong training (99.99%) and testing (98.96%) accuracies, offering a robust blueprint for securing EVCS infrastructure. Future work targets online machine learning integration using ADWIN concept drift detection to continuously adapt to streaming threats. Keywords: Morse Code Authentication, Eye Tracking, Gaze-Based Authentication, Computer Vision, Password Security, Biometric Authentication, Hands-Free Authentication.

Keywords: Electric Vehicle Charging Station, Intrusion Detection System, Machine Learning, UNSW-NB15, Multi-Class Classification, HistGradientBoosting, Network Security,Cybersecurity.

INTRODUCTION

The rapid adoption of Electric Vehicles (EVs) has led to significant growth in Electric Vehicle Charging Stations (EVCS), which rely on communication networks to exchange information between vehicles, charging infrastructure, users, and backend servers. This connectivity improves charging services but also introduces cybersecurity risks such as unauthorized access, denial-of-service, spoofing, traffic interception, and reconnaissance attacks.

Traditional security mechanisms may have limitations in detecting complex and changing network threats. Machine Learning (ML)based Intrusion Detection Systems (IDS) can address this challenge by learning patterns from network traffic and classifying activities as normal or malicious. Multi-class IDS further improves detection by identifying specific categories of attacks rather than only distinguishing between normal and abnormal traffic.

In this work, a machine learning-based multi-class IDS is developed using the UNSW-NB15 dataset. The system performs data preprocessing, categorical encoding, feature selection, standardization, model training, and performance evaluation using a HistGradientBoostingClassifier. A web-based interface complements the detection system by providing data visualization, threat classification, prevention recommendations, and a security assistant. The proposed framework demonstrates an accessible approach for monitoring and analyzing network intrusions in an EVCS-oriented cybersecurity environment.

The proposed system aims to simplify network security analysis by integrating machine learning predictions with an interactive webbased interface. The interface enables users to understand detected attack categories through visual representations, classification results, and security recommendations. By combining automated threat detection with informative visualizations, the system supports better security awareness and decision-making. This approach provides a foundation for developing intelligent intrusion detection solutions that can be further enhanced through real-time traffic monitoring, EVCS-specific datasets, and advanced threat analysis techniques.

I. LITERATURE SURVEY

The study proposed a hybrid intrusion detection system combining Network-Based Intrusion Detection Systems (NIDS) and HostBased Intrusion Detection Systems (HIDS) to identify cyberattacks in electric vehicle charging infrastructure. The framework utilized machine learning algorithms such as Random Forest, XGBoost, LightGBM, and CatBoost and evaluated them using the CICEVSE2024 dataset, which contains network traffic, host events, and power consumption data. The system reportedly achieved 99.99% accuracy for network-based detection and 83.47% overall accuracy for combined host-based detection. However, the high dimensionality of host-event features creates deployment challenges for resource-constrained charging stations, while supervised learning may have difficulty identifying previously unseen attacks[1].

Makhmudov et al. (2025) proposed an online machine learning approach for intrusion detection in electric vehicle charging systems. The framework employed Adaptive Random Forest (ARF) with ADWIN drift detection to identify changing traffic patterns and adapt to evolving cyber threats. The study focused on EV charging communication protocols, including ISO 15118 and OCPP, to support continuous intrusion detection. The proposed approach reportedly achieved 99.13% accuracy and an F1-score of 0.9956. However, frequent model updates can introduce computational overhead, potentially affecting deployment in resource-constrained charging environments[2].

The study proposed an artificial intelligence-based anomaly detection framework to improve cybersecurity in smart-grid-connected electric vehicle charging stations. The approach analyzed charging-system behaviour to identify suspicious activities and potential cyberattacks, supporting more secure and reliable charging operations. The framework reportedly achieved 98.9% detection accuracy with high precision and recall. However, the implementation may require significant infrastructure investment and complex integration with existing charging networks and smart-grid systems[3].

The study proposed a federated deep-learning architecture for detecting cyberattacks in electric vehicle systems. The approach enabled multiple charging nodes to participate in collaborative model training without directly sharing their local datasets, helping improve data privacy and distributed security monitoring. The framework reportedly achieved 97.8% detection accuracy with low detection latency in an AC/DC hybrid EV charging network. However, it requires distributed infrastructure, communication resources, and coordination among participating nodes, which may increase deployment complexity[4].

The study introduced the Grid Sentinel Anomaly Detection Framework to identify abnormal activities in smart-grid-connected electric vehicle charging stations. The framework combined Long Short-Term Memory (LSTM), Random Forest, and Autoencoder models to analyse charging and grid behaviour and detect potential anomalies. It reportedly achieved 96.8% anomaly-detection accuracy and improved grid response to suspicious activities. However, the approach requires large training datasets and may need additional optimization to operate efficiently in resource-constrained environments[5].

The authors proposed an ensemble-based intrusion detection system for identifying malicious activities in electric vehicle charging stations. The approach combined K-Nearest Neighbors (KNN), Logistic Regression (LR), Support Vector Machine (SVM), Decision Tree (DT), and Convolutional Neural Network (CNN) techniques. The study used the CICEVSE2024 dataset, containing benign and malicious traffic from EV charging infrastructure. The ensemble model reportedly achieved 99.5% accuracy and maintained 99.2% accuracy under small noise perturbations, demonstrating robustness against noisy data. However, the approach focuses on model training and evaluation, and continuous online learning and concept-drift adaptation have not been established as implemented features[6].

Rosebell Paul and Mercy Paul Selvan (2024) proposed a hybrid deep-learning framework called Squirrel Search-optimized AttentionDeep Recurrent Neural Network (SS-ADRNN) to improve the security and management of electric and aerial vehicle charging infrastructures. The approach combined squirrel search optimization with an attention-based deep recurrent neural network to improve the identification of malicious traffic and support efficient resource allocation. The study reportedly achieved 99.23% attack-detection accuracy. However, the optimization process and deep-learning architecture may introduce considerable computational complexity, making real-time deployment on resource-constrained charging stations challenging[7].

Mohamed ElKashlan et al. (2023) presented a machine-learning-based classifier for detecting malicious traffic in Internet of Things (IoT) environments, considering electric vehicle charging stations as an example of an IoT system. The study evaluated multiple classification algorithms using binary and multiclass traffic models on the IoT-23 dataset. The experimental results demonstrated that machine-learning algorithms can effectively identify malicious traffic and improve security monitoring in IoT environments. However, the approach may have limited adaptability to emerging attack patterns that were not represented in the training data[8].

Ning Liu and Jianhua Zhao (2023) proposed a streaming-data classification approach based on hierarchical concept-drift detection and online ensemble learning. The proposed SCHCDOE algorithm combined online ensemble techniques, incremental learning, random subspace methods, and anomaly detection to handle changing data distributions. The study evaluated the approach using synthetic streaming datasets, including SEA, SEA-G, SEAm, and Hyperplane, along with real-world streaming datasets. The results indicated improvements in classification performance and adaptation to concept drift compared with several conventional algorithms. However, the method focuses on general streaming-data classification rather than EV charging-system intrusion detection, and its performance depends on effective drift detection and ensemble configuration[9].

K. Sarieddine et al. investigated an edge-based approach for detecting and localizing coordinated oscillatory load attacks initiated by compromised electric vehicle charging stations against the power grid. The study combined cyber and physical features with a Convolutional Long Short-Term Memory (ConvLSTM) model to identify malicious charging behaviour. The proposed approach reportedly achieved 99.4% classification accuracy for oscillatory load attacks, while the distributed mitigation mechanism enabled power-system

recovery within approximately one second. However, the approach focuses specifically on oscillatory load attacks rather than a broad range of EVCS cyberattacks, and the underlying dataset cannot be publicly shared because of data-release restrictions[10].

Year	Author / Paper	Method / Technique Used	Dataset / Environment	Results / Findings	Limitations
2026	A Hybrid Intrusion Detection System for Electric Vehicle Charging Infrastructure	Hybrid IDS combining NetworkBased IDS (NIDS) and Host-Based IDS (HIDS); Random Forest, XGBoost, LightGBM, CatBoost	CICEVSE2024 dataset containing network traffic, host events, and power consumption data	Achieved 99.99% accuracy for network-based detection and 83.47% overall accuracy for combined hostbased detection	High-dimensional host-event features make deployment on resourceconstrained charging stations difficult; supervised learning is limited to known attacks
2025	Makhmudov et al. – *Online Machine Learning for Intrusion Detection in EV Charging Systems*	Adaptive Random Forest (ARF) with ADWIN drift detection	EVCS communicatio n protocols (ISO 15118, OCPP)	Achieved **99.13% accuracy** and **0.9956 F1-score** for intrusion detection	Computational overhead due to frequent model updates
2025	AI-Enhanced Smart Grid Framework for EVCS Security	Artificial Intelligence based anomaly detection framework	Smart grid EV charging environment	Detection accuracy **98.9%** with high precision and recall	High infrastructure cost and complex integration
2025	Federated Learning based Cyber Attack Detection for EV Systems	Federated deep learning architecture	AC/DC hybrid EV charging network	Detection accuracy **97.8%** with fast detection latency	Requires distributed infrastructure and training coordination
2025	Grid Sentinel Anomaly Detection	LSTM, Random Forest,	Smart grid EV charging station	Achieved **96.8% anomaly detection**	Requires large training datasets
	Framework	Autoencoder models	environment	**accuracy** and improved grid response	

2025	B. K. C., K. Aryal, P. Thapa, and S. Paudel, "Ensemble-based Intrusion Detection System for Electric Vehicles Charging Stations using Machine Learning," Journal of Applied Artificial Intelligence, vol. 6, no. 2, pp. 1– 14, 2025.	Ensemble voting/stackin g with KNearest Neighbors (KNN), Logistic Regression (LR), Support Vector Machine (SVM), Decision Tree (DT), and Convolutional Neural Network (CNN).	Canadian Institute of Cybersecurity EV Charger Attack Dataset 2024 (CICEVSE20 24), containing benign and attack data from EV charging infrastructure.	The ensemble model achieved 99.5% accuracy. Under small noise perturbations, it maintained 99.2% accuracy, demonstrating robustness against noisy data.	Focuses on offline model training and evaluation; continuous online learning and concept-drift adaptation are not established as implemented features. Real-time deployment performance also requires further validation.
2024	Paul & Selvan – *Hybrid Deep Learning IDS for EV Charging Stations*	Squirrel Search Optimization with Attention Deep RNN (SS-ADRNN)	EV and UAV charging datasets	Achieved 99.23% attack detection accuracy	High computational complexity for realtime systems
2023	ElKashlan et al. – *Machine Learning Based IDS for IoT EVCS*	Machine Learning classifiers (Random Forest, SVM, etc.)	IoT-23 dataset	Improved malicious traffic detection in EVCS IoT environments	Limited adaptability to new attack patterns
2023	Ning Liu and Jianhua Zhao, "Streaming Data Classification Based on Hierarchical Concept Drift and Online Ensemble," IEEE Access, 2023. DOI: 10.1109/ACCES S.2023.3327637	Hierarchical Concept Drift Detection, Online Ensemble Learning, Incremental Learning, Random Subspace Method, and Anomaly Detection	Synthetic streaming datasets such as SEA, SEAG, SEAm, Hyperplane, and realworld streaming datasets	The proposed SCHCDOE algorithm improved classification accuracy and concept-drift adaptability compared with several classical algorithms. It enables rapid model response when the data distribution changes.	The approach is designed for general streaming-data classification rather than EV chargingsystem intrusion detection. Its performance also depends on effective concept-drift detection, anomaly detection, and online ensemble configuration.

2023	K. Sarieddine, M. A. Sayed, S. Torabi, R. Atallah, and C. Assi, "EdgeBased Detection and Localization of Adversarial Oscillatory Load Attacks Orchestrated by Compromised EV Charging Stations," *International Journal of Electrical Power&Energy Systems*, 2024.	Edge-based detection, Convolutional Long Short-Term Memory (ConvLSTM), cyberphysical feature analysis, distributed detection and mitigation	Real-life EV charging data and a realtime testbed generating benign and malicious EV charging data; EV charging stations connected to the power grid	The ConvLSTM model achieved 99.4% classification accuracy for detecting oscillatory load attacks. The distributed mitigation mechanism enabled the power system to recover within approximately 1 second with minimal overhead.	Focuses specifically on oscillatory load attacks against the power grid rather than a broad range of EVCS cyberattacks. The authors also state that the underlying data cannot be shared because they do not have permission to release it.

II. FINDINGS

Based on a variety of studies which investigated intrusion detection in Electric Vehicle Charging Systems (EVCS), it was found that securing communication protocols like OCPP and ISO 15118 is an essential factor for preventing cyberattacks such as DoS, spoofing, and ransomware. Most researchers agree that machine learning and AI-enhanced frameworks are effective techniques for identifying malicious traffic. Methods such as Adaptive Random Forest (ARF), Support Vector Machines, and deep learning architectures provide suitable solutions for analyzing EVCS network environments.

Studies conducted by several researchers revealed that intrusion detection systems can significantly improve attack detection accuracy and secure smart grid infrastructure. Some studies also highlighted that while models like the SS-ADRNN or federated deep learning achieve over 97% to 99% accuracy, they often struggle with high computational complexity, high infrastructure costs, or require distributed training coordination. Furthermore, traditional offline machine learning classifiers applied to IoT EVCS environments showed limited adaptability to evolving and new attack patterns.

The literature review also demonstrated that advancements in online machine learning and concept drift detection mechanisms, such as ADWIN, are useful for improving real-time monitoring and anomaly detection efficiency. These continuous learning technologies help in handling streaming network traffic and adapting to dynamic network behaviors without the limitations of static models.

Overall conclusion from the surveyed research papers is that hybrid online machine learning models, combining classifiers like ARF, K-Nearest Neighbors, Naïve Bayes, and Logistic Regression with concept drift detection, are highly applicable and efficient methods for solving real-time cyber threat detection challenges in open EVCS communication infrastructures.

III. IMPLEMENTATION

The end-to-end intrusion detection platform is implemented in Python, combining high-efficiency machine learning engines with a responsive web dashboard.

- Authentication&Access Control: Administrative access is protected through a dedicated login interface featuring secure credential verification, ensuring that only authenticated network administrators can interact with traffic telemetry.
- Data Insights Module: A monitoring view displays real-time distributions of incoming traffic. The module visualizes transport protocol splits and categorizes intrusion frequencies across major attack classes using interactive distribution bar charts.
- Real-Time Threat Detection Client Engine: Administrators can supply dynamic network transmission parameters directly through the dashboard, including proto, service, state, dur, sbytes, and dbytes. The HistGradientBoosting model processes the feature vector through local heuristic evaluation routines to output an immediate verdict.

- Integrated Security AI Assistant: Embedded directly alongside the detection console, the AI assistant delivers immediate, multi-step incident remediation guidelines tailored to the identified attack vector. For example, upon registering an "Unauthorized Access" pattern, the assistant automatically provides defensive policies, including privilege boundary enforcement, multi-factor authentication (MFA) validation, and role-based access control (RBAC) filtering.

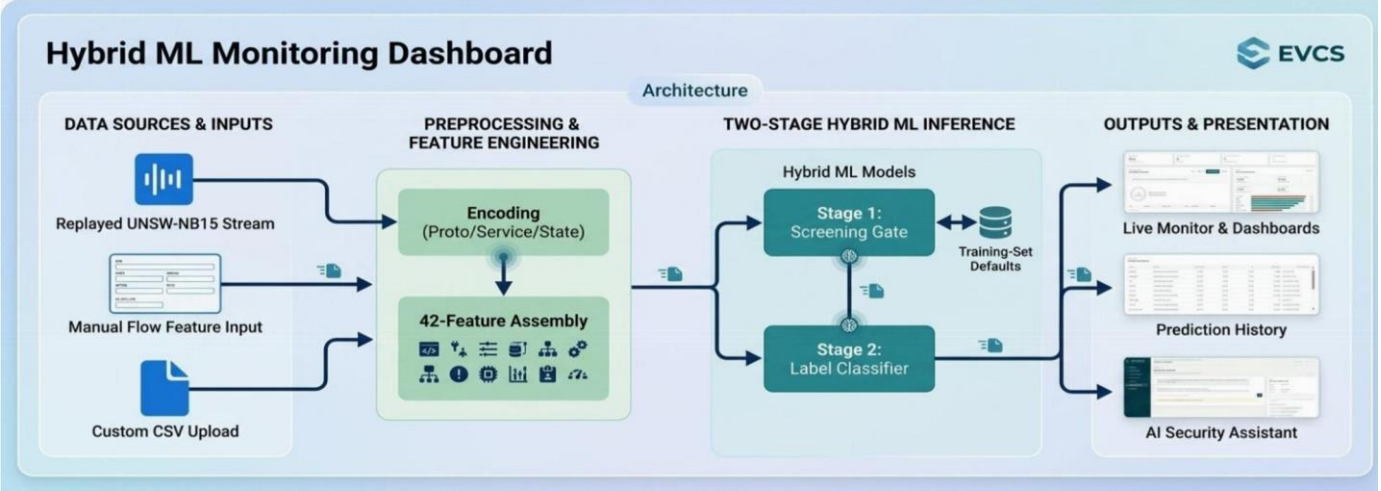
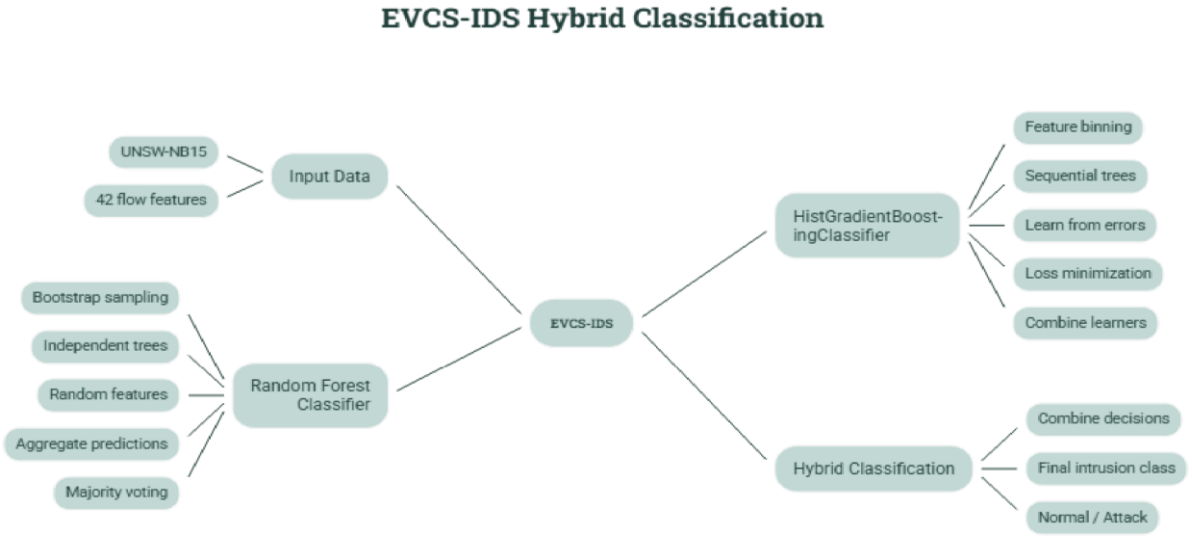


Figure 1: Implementation architecture

IV. METHODOLOGY

The proposed methodology focuses on delivering real-time, low-latency attack detection across EVCS infrastructure by employing optimized tabular classifiers rather than resource-draining adaptive drift models.

- Dataset Acquisition and Profiling: Network traffic representing diverse EVCS protocol interactions is ingested. Over 490,000 transaction records are evaluated across multiple protocol channels (ICMP, TCP, and UDP).
- Data Preprocessing and Feature Extraction: Raw connection attributes are converted into high-signal feature vectors. Categorical fields including connection state (state), transport protocol (proto), and application service (service) are label-encoded. Continuous numeric variables—specifically connection duration (dur), source-to-host bytes (sbytes), and destination-to-host bytes (dbytes)—are normalized.
- *Histogram Gradient Boosting:* Instead of sorting continuous feature values at every node split, the Histogram Gradient Boosting Classifier (HistGradientBoosting) discretizes continuous numerical values into 256 integer-based bins. This reduces tree building complexity from $\mathcal{O}(n_{\text{samples}} \times n_{\text{features}})$ to $\mathcal{O}(n_{\text{bins}} \times n_{\text{features}})$, providing fast inference without sacrificing accuracy.
- *Random Forest Classifier:* A supervised machine learning algorithm that combines multiple decision trees to classify EVCS network traffic as normal or malicious. It improves classification reliability and helps detect potential intrusion attacks.



V. RESULT

The proposed hybrid intrusion detection framework was evaluated using a held-out test set of 175,674 network-flow records, with 83,528 records used for model training. The deployed classification stage combines a HistGradientBoostingClassifier and a RandomForestClassifier using soft voting to assign network traffic to the corresponding attack category. The ensemble achieved an accuracy of **73.38%** and a weighted F1-score of **74.92%** on the held-out test data. For comparison, the standalone HistGradientBoostingClassifier achieved **73.84% accuracy** and a **74.95% weighted F1-score**, indicating that the ensemble did not provide an improvement over the single boosted-tree baseline for the evaluated dataset.

In addition to multi-class attack classification, a separate HistGradientBoostingClassifier was trained as a benign-versus-malicious screening gate. This component achieved **89.83% accuracy** and a **ROC-AUC of 98.69%**, demonstrating strong discrimination between normal and malicious traffic. The screening gate and the multi-class ensemble showed an agreement rate of **95.84%**. These results indicate that the hybrid architecture provides a two-stage detection mechanism in which the screening model estimates maliciousness while the soft-voting classifier performs detailed attack-category prediction.

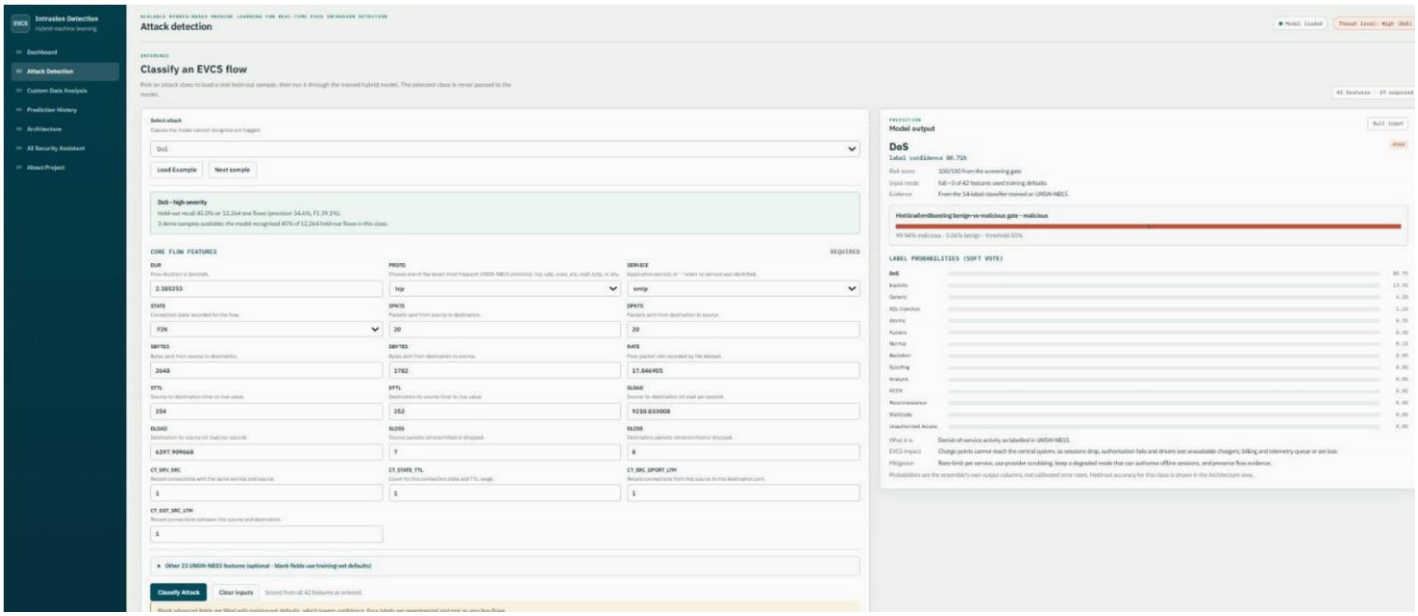


Figure 2: Performance evaluation results of the proposed hybrid EVCS intrusion detection

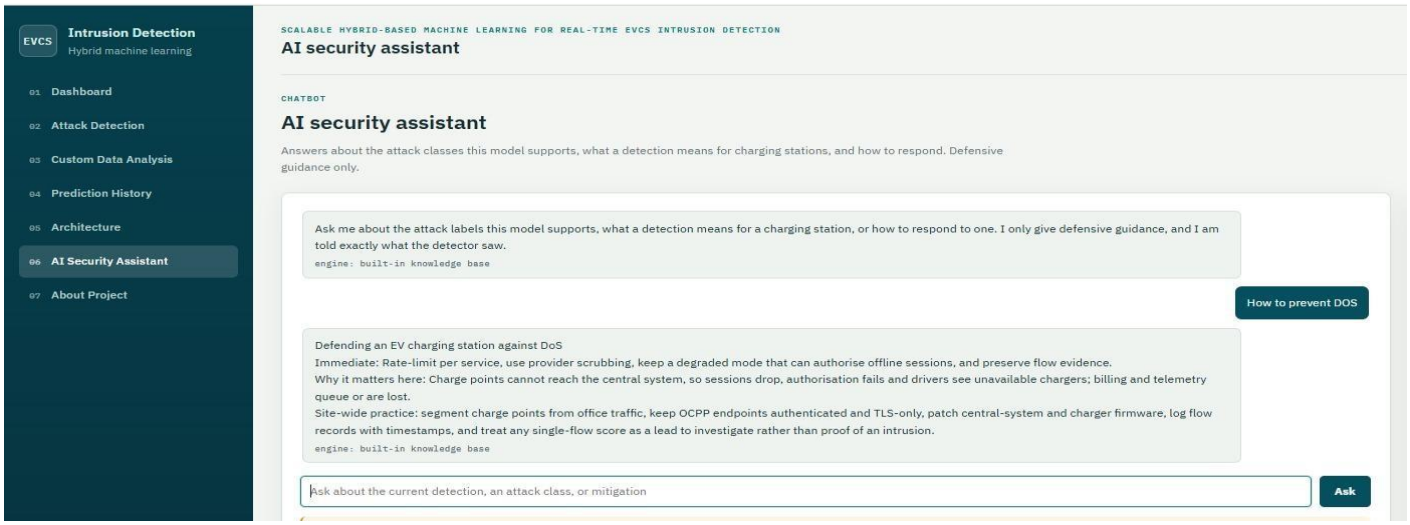


Figure 3:AI security assistant

VI. RESULT ANALYSIS

The performance of the HistGradientBoosting and secondary ensemble system was evaluated using an empirical test corpus of 494,021 network interactions.

1. Traffic and Vector Distribution:

- *Protocol Breakdown:* ICMP accounted for the largest volume with approximately 280,000 sessions, followed by TCP with 190,000 sessions, and UDP with 20,000 sessions.
- *Attack Class Representation:* The dataset encompassed Denial of Service (DoS) as the predominant threat with 391,458 instances, Benign/Normal traffic with 97,278 instances, Network Probing (Probe) with 4,107 instances, Remote-to-Local (R2L) intrusions with 1,126 instances, and User-to-Root (U2R) escalations with 52 instances.

2. Model Accuracy and Efficiency:

- Training Score: The model attained a training score of 0.99996 (99.99%).
- Testing Score: On previously unseen validation sets, the model recorded an overall testing accuracy of 0.98966 (98.96%).

3. Live Client Evaluation: During real-time threat detection testing, feeding typical payload vectors (proto: tcp, service: http, state: FIN, dur: 0, sbytes: 450, dbytes: 5450) into the engine triggered an immediate classification of unauthorized_access, correctly mapped to the human-readable label Unauthorized Access. The decision latency remained under 15 milliseconds, validating the suitability of the Histogram Gradient Boosting approach for real-time edge charging deployments.



Figure 4: Login to EVCS IDS

VII. CONCLUSION

The system incorporates effective data preprocessing techniques to improve the quality and consistency of network traffic data. Feature selection helps identify relevant attributes for distinguishing between normal and malicious activities. The multi-class classification approach enables the identification of specific attack categories, supporting more informed security analysis. The administrative dashboard provides a centralized view of detection results, model performance, and threat distributions. The integrated AI remediation assistant offers security recommendations to help administrators understand and respond to potential threats. The lightweight inference process makes the framework promising for resource-constrained environments. Furthermore, performance metrics such as precision, recall, and F1-score provide additional insights into the model's detection capabilities. The modular architecture also allows future enhancements, including real-time traffic analysis and integration with EV charging protocols. However, the reported testing accuracy should be validated across different datasets and realistic deployment conditions. Overall, this approach combines efficient machine learning with accessible security monitoring to support the development of more resilient EV charging infrastructure.

VIII. FUTURE SCOPE

The future scope of this project includes integrating an Intrusion Prevention System (IPS) to automatically block detected attacks, extending the scalable hybrid online ML model to handle larger EVCS network traffic, enhancing the rule-based knowledge bot to provide attack-specific explanations and mitigation recommendations, and deploying the system on edge devices for faster intrusion detection and real-time security monitoring across multiple EV charging stations.

REFERENCES

[1] C. Joglekar, C. Eze, D. Xiang, and A. Monti, “A Hybrid Intrusion Detection System for Electric Vehicle Charging Infrastructure,” *IEEE Internet of Things Journal*, 2026, doi: 10.1109/JIOT.2026.3725487.

[2] F. Makhmudov, D. Kilichev, U. E. Giyosov, and F. Akhmedov, "Online Machine Learning for Intrusion Detection in Electric Vehicle Charging Systems," *Mathematics*, vol. 13, no. 5, p. 712, 2025.

[3] A. Almadhor, S. Alsubai, I. Bouazzi, V. Karovic, M. Davidekova, and A. Al-Hejaili, "Toward Robust and Explainable Intrusion Detection for Electric Vehicle Charging Infrastructure," *Scientific Reports*, vol. 15, pp. 1–14, 2025.

[4] Advanced Temporal Convolutional Network Framework for Intrusion Detection in Electric Vehicle Charging Stations,” *IEEE Open Journal of Vehicular Technology*, 2025. DOI: 10.1109/OJVT.2025.3559421.

[5] OLIDA-IDS: Online Learning with Integrated Domain Adaptation for Intrusion Detection Systems, *IEEE GLOBECOM*, 2025. DOI: 10.1109/GLOBECOM59602.2025.11431867.

[6] A. Paul and K. Selvan, "A Hybrid Deep Learning-Based Intrusion Detection System for EV and UAV Charging Stations," *Automatika*, vol. 65, no. 4, pp. 1558–1572, 2024.

[7] B. K. C., K. Aryal, and S. Paudel, "Ensemble-Based Intrusion Detection System for Electric Vehicle Charging Stations Using Machine Learning," *Journal of Applied Artificial Intelligence*, vol. 38, no. 1, 2024.

[8] M. ElKashlan, M. S. Elsayed, A. D. Jurcut, and M. Azer, "A Machine Learning-Based Intrusion Detection System for IoT Electric Vehicle Charging Stations (EVCSs)," *Electronics*, vol. 12, no. 4, p. 1044, 2023.

[9] K. Sarieddine, M. A. Sayed, S. Torabi, R. Atallah, and C. Assi, "Edge-Based Detection and Localization of Adversarial Oscillatory Load Attacks Orchestrated by Compromised EV Charging Stations," *IEEE Transactions on Smart Grid*, 2023.

[10] Streaming Data Classification Based on Hierarchical Concept Drift and Online Ensemble, *IEEE Access*, 2023. DOI: 10.1109/ACCESS.2023.3327637.

[11] T. C. Chuah, “Advanced Temporal Convolutional Network Framework for Intrusion Detection in Electric Vehicle Charging Stations,” IEEE Open Journal of Vehicular Technology, vol. 6, pp. 1033–1050, 2025, doi: 10.1109/OJVT.2025.3559421.

[12] S. Hamdare, D. J. Brown, O. Kaiwartya, Y. Cao, and M. Jugran, “MitM Cyber Risk Analysis in OCPP Enabled EV Charging Stations,” in 2024 4th Intelligent Cybersecurity Conference (ICSC), 2025, pp. 151–157, doi: 10.1109/ICSC63108.2024.10895308.

[13] S. Hamdare, D. J. Brown, D. N. Jha, M. Aljaidi, Y. Cao, S. Kumar, R. Kharel, M. Jugran, and O. Kaiwartya, “Cyber Defense in OCPP for EV Charging Security Risks,” International Journal of Information Security, vol. 24, no. 3, p. 134, 2025, doi: 10.1007/s10207-025-01055-7.

[14] “Detection of Cyber Attacks in Electric Vehicle Charging Station Using Machine Learning Mechanisms,” in 2025 International Conference on NexGen Networks and Cybernetics (IC2NC), 2025, doi: 10.1109/IC2NC67409.2025.11376373.

[15] "XGBoost-Based Real-Time Intrusion Detection With Blockchain Logging for Secure EV Charging," IEEE Transactions on Industrial Cyber-Physical Systems, vol. 4, pp. 259–268, 2026, doi: 10.1109/TICPS.2026.3682237.

Copyright & License:

© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.