Comparative Evaluation of Supervised Machine Learning Algorithms for Intrusion Detection in Electric Vehicle Systems

Carlos Noboyuki Noda Junior
São Paulo State Univ. of Tech. (FATEC)
Ourinhos, Brazil
carlos.junior@fatecourinhos.edu.br

Thiago José Lucas
São Paulo State Univ. of Tech. (FATEC)
Ourinhos, Brazil
thiago@fatecourinhos.edu.br

Fernanda Mara Cruz
São Paulo State Univ. of Tech. (FATEC)
Ourinhos, Brazil
fernanda.cruz@unesp.br

Eduardo Alves Moraes
São Paulo State University (UNESP)
Bauru, Brazil
eduardo.moraes@unesp.br

Alessandra de Souza Lopes
São Paulo State University (UNESP)
Bauru, Brazil
alessandra.lopes@unesp.br

Kelton Augusto Pontara da Costa
São Paulo State University (UNESP)
Bauru, Brazil
kelton.costa@unesp.br

***Abstract*—With the growth of the electric car (EC) industry and market, it is natural that the use of cutting-edge technologies to provide inter-connectivity between cars and other devices will be implemented in their structures, both in the cars themselves and in their essential products, such as chargers. Given that such technologies open up opportunities for attacks on the cars' critical infrastructure, the damage resulting from an eventual attack proves to be a major challenge for the cybersecurity area. Motivated by this scenario, this article proposes the development of an analysis of machine learning models for intrusion detection systems (IDS), to protect electric cars against intrusions. Most models achieved high accuracy, precision, recall, and F1-scores, with RNN LSTM leading in performance (0.999) despite higher computational cost. At the same time, Random Forest, AdaBoost, and CN2 offered strong results with lower training time, Naive Bayes proved efficient for limited resources, and Logistic Regression showed the weakest performance.**

***Keywords*—Electric Vehicle, Machine Learning, Intrusion Detection System, Cybersecurity, CAN Bus.**

I. Introduction

The human need for independence from oil has been growing in several industries, particularly the automotive sector. This is evidenced by the growth of the global electric vehicle (EV) market. In 2024, more than one-fifth (exceeding 20%) of the total number of automobiles sold worldwide were electric vehicles, as pointed out by [1].

The adoption of technology also extends to the critical infrastructure on which EVs depend, such as high-capacity chargers, which can reduce charging time to as little as one hour, making the process more efficient for the end user, as stated by [2]. Furthermore, EVs are mostly equipped with various state-of-the-art technologies, both for user comfort and for vehicle operation. For these technologies to be optimized, data collection is required, which may include everything from internal telemetry obtained by the vehicle's sensors to confidential information about the driver. These data can be obtained through connected services in the EV and the owner's mobile phone via Bluetooth, as well as through third-party applications such as Google Maps, as noted by [3].

The aforementioned technologies require communication and data exchange to operate normally, creating a concerning amalgam of sensitive information transiting in an open environment, with a direct connection between two hardware components (car and charger) that may contain potential vulnerabilities.

EVs and their chargers feature auxiliary software within their infrastructure to help maintain physical integrity, energy flow, and inter-connectivity between charger and vehicle. By design, these chargers must be connected to the internet, which creates a vulnerable point for the security of both vehicle and charger data, as stated by [4]. When the car is being charged, a physical connection occurs between the charger and the vehicle. If not properly protected, both the physical integrity of the vehicle and the user information generated in this process are put at risk.

Electric vehicle connectors are potential targets for attackers due to their communication protocols and connectivity capabilities. These vulnerabilities can be exploited to introduce malware or manipulate billing settings, allowing unauthorized access to the charging station. This scenario emphasizes the

need for stronger security measures in EV charging ecosystems.

Consequences of an inadequately protected electric vehicle infrastructure can pose serious risks to the confidentiality of sensitive driver and manufacturer data. They can also affect the power grid, leading to disruptions in its proper operation, as mentioned by [5]. Direct damage to the driver and the integrity of the EV is also a real possibility. If an EV's ACC (adaptive cruise control) sensor — responsible for the vehicle's acceleration and braking — is compromised, the EV could accelerate or brake without driver intent, causing dangers and harm to both driver and vehicle, as [6] describes.

Given the growing importance of EVs and the vast amount of data they generate, the Research Problem that motivates the efforts employed in developing this scientific work arises: is there performance feasibility (processing time for detection and attack detection rate) in creating an IDS for EV protection?

In light of the vulnerabilities in EV connectors, this scientific work proposes the development of an intrusion detection system (IDS) that integrates machine learning techniques. The integration of machine learning aims to improve intrusion detection performance, being an essential technology for cybersecurity and related industrial sectors. To achieve the project's general objective, various machine learning models — Random Forest, Decision Tree, Naive Bayes, AdaBoost, Logistic Regression, RNN LSTM, and CN2 Rule Induction — were evaluated to identify the one offering the best balance between detection accuracy and computational cost. Neural networks stand out for delivering excellent results and are widely used in IDS systems, as noted by [7], even though they require greater computational resources. The system implementation will be carried out in Python, chosen both for its wide range of libraries for machine learning development and for the familiarity with the language due to prior experience. The models will be trained using the CICIoV2024 dataset, with more details about dataset selection and algorithm choice provided in section III.

The goal is, therefore, to achieve an optimized balance between robust threat detection performance and the necessary energy efficiency — a crucial consideration in the selection and implementation of machine learning models for this application.

This article is structured to clearly and systematically present the fundamentals and results obtained. After this introduction, Section II addresses the theoretical framework, discussing the main vulnerabilities and security challenges in electric vehicles and their charging infrastructures. Section III details the methodological procedures adopted, including dataset selection, preprocessing techniques, and a description of the machine learning algorithms used. Section IV presents and discusses the results obtained, comparing the performance and computational cost of the evaluated models. Finally, Section V summarizes the study's conclusions and proposes directions for future research.

II. Theoretical Background

Electric cars and their charging ecosystems present an expanded attack surface, as they integrate internal buses (such as CAN) with external interfaces, telematics, and cloud-connected charging infrastructure. In-vehicle, the CAN protocol lacks authentication and encryption, enabling message injection, spoofing, and DoS if an attacker gains logical or physical access — something already widely explored in onboard intrusion detection studies [8]. Outside the vehicle, smart charging infrastructure and charging management introduce additional vectors: attacks against communication protocols (e.g., OCPP), manipulation of charging profiles, and exploitation of integration with backend applications and services, with potential functional security and privacy impacts. Recent reviews highlight that, although newer versions of OCPP strengthen security mechanisms, gaps and operational challenges persist in its widespread adoption [9].

The vulnerability is not limited to the individual vehicle and charging station: EV-charger-grid coupling creates cyber-physical interdependencies that can be exploited for systemic effects (e.g., malicious demand shifting, coordinated disruptions, or feeder overloading). IEEE benchmark studies show that smart charging security is critical to grid resilience, mapping backdoors in assets, interfaces, and operational data, and discussing how attacks on charging orchestration can propagate from the station to the electrical system [10], in addition to highlighting new vectors when public/operational station data is combined with PEV usage profiles [11]. These findings reinforce that EV security is simultaneously an automotive IT problem and a critical infrastructure issue.

In this scenario, the implementation of intrusion detection systems (IDS) is crucial both onboard the vehicle and at the edge of the charging infrastructure. In-vehicle, deep learning-based IDSs (e.g., LSTM models) have demonstrated high accuracy in identifying anomalies in CAN traffic without the need to decode payloads, detecting DoS attacks, fuzzing, and spoofing in near-real time [8]. On the charger and backend side, reviews of the OCPP and the charging ecosystem recommend continuous monitoring, secure telemetry, and event correlation (charger to CSMS to network) to detect state, firmware, and charging session manipulations [9], [10]. Together, onboard IDSs and infrastructure IDSs form a defense in depth that reduces the window of exposure, accelerates incident response, and improves the operational resilience of the electric mobility system.

A. Correlated Work

In [12], the emphasis is placed on further strengthening protection in IoT systems, focusing on the use of Z-score standardization and Min-Max normalization on existing datasets. Recognizing the importance of proper preprocessing — both for the model's results and for its reliability — this scientific publication contributes to the foundation of the preprocessing phase for the chosen dataset. Although the study in question works with different datasets, these are still renowned and are frequently used in several other studies.

It is of utmost importance to have a high-level perspective on embedded technologies in EVs, thereby facilitating the understanding of existing vulnerabilities in EVs today and identifying future market trends. The study by [2] reviews current and future high-speed charging technologies, specifically discussing what is referred to in the study as ultra-fast charging. The authors address state-of-the-art chargers, charging standards, and the essential infrastructure of chargers and EVs.

In [4], the authors consider the expansion of EV infrastructure, the need for security in such infrastructure, and its proper functioning. They propose various ML algorithms for detecting malicious traffic in IoT environments, using the IoT-23 dataset — specialized for IoT — to protect EV chargers, which also operate based on IoT systems. The classifiers tested were: Naïve Bayes, J48 classifier, Attribute Select, and Filtered Classifier. Among these, the Filtered Classifier achieved the best results, with 98.00% F1-score and 99.00% precision.

[13] developed an IDS for electric vehicles focused on detecting DoS and DDoS attacks, providing greater insight into vulnerabilities in EV infrastructure. The authors implemented two hybrid models working together: a Deep Neural Network (DNN) and a Long Short-Term Memory (LSTM). The study used the CICIDS 2018 dataset, which influenced the choice of the dataset used in the current research — produced by the same institution — as well as the choice of classifier algorithm. By employing two deep learning classification algorithms in combination, the study achieved high performance, with both F1-score and precision reaching 99.00%, but at the cost of high computational power requirements and longer model training time.

The scientific study by [14] provides an in-depth analysis of the current state of security and threats for electric vehicles, highlighting technological market trends. The main focus of the paper is the vulnerabilities in EV-related infrastructure (such as chargers and communication protocols), which are emphasized and provide a clear overview of the current security scenario for EVs and their infrastructure, as well as offering solutions to these vulnerabilities. The study discusses risks associated with charging protocols involving EV-to-charger communication and the types of attacks EVs may be susceptible to, such as malware injection, false data injection, Man-in-the-Middle, and DoS. This study was instrumental in providing a broader understanding of the current security state of EVs.

According to [15], the evaluation of machine learning classifiers is proposed for an intrusion detection system with a greater focus on the CAN bus, a communication protocol that enables multiple microcontrollers and devices to communicate — a critical component and frequent target of attacks due to the nature of the data it transmits and its lack of built-in security. The publication compares the performance of several classifiers, including Support Vector Machine, Decision Tree, Random Forest, and Multilayer Perceptron, against various CAN bus attacks, such as DoS, with all tests conducted on a real vehicle. Its contribution lies in improving the understanding of the CAN bus, which, while crucial to EV operation, is also vulnerable in most cars. The best-performing model in comparison was Random Forest, with a 98.00% F1-score and 97.20% accuracy.

The authors of [16] highlight the importance of reinforcing security in internal EV components, such as the previously mentioned CAN bus. With this problem established, they propose the creation of a network-based IDS variant, named OMIDS, working together with a machine learning model. The classifier algorithm used was VGG16, a Convolutional Neural Network model for attack identification, which in the study was compared to another classifier called XBoost, an ensemble learning model. Final results showed that XBoost achieved a 98.24% F1-score and 95.95% precision, making it the superior model in the comparison.

[5] highlights how compromised IoT devices can be used to manipulate power grid demand to levels far beyond normal. A large IoT device botnet, referred to in the study as "MadIoT," can cause severe damage to the power grid, including blackouts, instability, and overloading of power lines. Since electric vehicles also fall into the IoT device category, the publication was valuable in demonstrating how EVs could be part of such an attack, amplifying their damage and efficiency due to their high voltage during charging.

Following this, the research by [6] discusses the significance of sensors for EV operation, both in their role for sustainability and for providing operational services and driver comfort. However, these same sensors introduce vulnerabilities, making EVs susceptible to a wide range of attacks, such as malware injection, interference with sensor operation, and data extraction. Understanding the role of EV sensors and their weaknesses was crucial, as was exploring defensive measures against these identified threats.

In [7], a comprehensive analysis of neural network use in IDSs is conducted. The authors explore advances in artificial

intelligence, focusing on the application of neural networks for network security and data privacy. The article covers several neural network architectures used in IDSs, such as multilayer perceptrons (MLPs), recurrent neural networks (RNNs), and convolutional neural networks (CNNs). This study provided deeper insight into neural networks for IDSs, thereby improving the understanding of the algorithm to be used for the EV IDS.

The study by [17] presents the creation of an IDS for autonomous EVs, arguing their higher risk and greater need compared to other IoT devices and vehicles of the same class, to enable real-time threat detection. Various types of classifier algorithms were evaluated, leading to the identification of the one with the best overall performance. After simulations, it was determined that Extreme Gradient Boosting was the top-performing classifier, with both F1-score and precision reaching 99.00

In the article by [18], the use of a deep learning model is proposed for detecting cyberattacks on Electric Vehicle Charging Stations (EVCS). Using the CICEVSE2024 dataset, the hybrid CNN-LSTM model developed demonstrated significant improvement over the original dataset study, achieving 97.15% accuracy, 97.19% precision, 97.15% recall, a 97.15% F1-score, and an area under the curve (AUC) of 97.14%. Additionally, the study employed the SHAP explainability technique, revealing the significant impact of 12 selected features in detecting benign and attack traffic.

In the study by [19], an online intrusion detection system for EVCS is presented, using an Adaptive Random Forest (ARF) classifier with Adaptive Windowing (ADWIN) drift detection to identify threats in real time and evolving environments. Evaluated with the CICEVSE2024 dataset, the model achieved, for binary intrusion detection, 99.13% accuracy, 99.99% precision, 99.14% recall, and a 99.56% F1-score, maintaining an average accuracy of 0.99 during drift events. In multiclass detection, the system obtained 98.40% accuracy, precision, and recall, with a 98.31% F1-score and an average accuracy of 0.96 during drift events.

B. Taxonomy of Correlated Work

This section presents the taxonomy of the cited works, which is essential for understanding the depth of the analysis conducted on intrusion detection systems applied to electric vehicles (EVs). In the search for more robust and efficient approaches, the reviewed studies explored a wide variety of datasets, machine learning algorithms, and evaluation metrics. This section provides an overview of the main contributions of these works, highlighting their methodologies, datasets, and performance outcomes, as summarized in Table I.

The taxonomy also reveals that, despite the increasing number of studies on cybersecurity for EVs and charging infrastructures, few works present a comparative evaluation of multiple machine learning algorithms applied specifically to intrusion detection in this context. This gap highlights the relevance of the present study, which proposes a systematic comparative analysis of different supervised classifiers for IDS in EVs, aiming to identify the most effective balance between detection accuracy and computational cost.

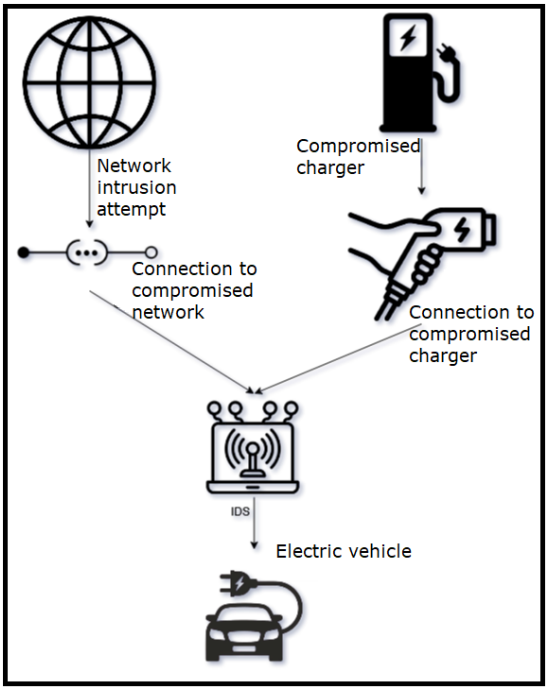

Fig. 1. Diagram of the structure of an attack on the vital infrastructure of an electric vehicle, and how the IDS can protect the EV.

III. Methodology

This study was conducted entirely with free software: all experiments were run on a Debian 12 Linux server using the scikit-learn library in Python. The research has a quantitative and experimental nature, dealing with large volumes of data and involving the creation of an ML model for an intrusion detection system aimed at protecting EVs, operating alongside a neural network classifier. The motivation for this choice is discussed in III-C, while the dataset processing is detailed in III-A. The details for each of the processes are specified below:

A. Dataset

Based on the information provided by the theoretical framework research, it was concluded that the most suitable dataset for the project is *CICIoV2024*, a dataset made available by the Canadian Institute for Cybersecurity (CIC), focused on the

Table I
SUMMARY OF RELATED WORKS ON EV INTRUSION DETECTION SYSTEMS

Work	Dataset	Classifiers	Results
[2]	N/A (technology review)	N/A	Analysis of ultra-fast charging technologies and EV infrastructure
[4]	IoT-23	Naïve Bayes, J48, Attribute Select, Filtered Classifier	Best: Filtered Classifier — F1 98%, PR 99%
[5]	N/A (IoT botnet)	N/A	Demonstrates risk of IoT-based attacks, including EVs, on the power grid
[6]	N/A (EV sensors)	N/A	Identification of vulnerabilities in EV sensors and defensive measures
[7]	N/A (neural network review)	MLP, RNN, CNN	Insights into neural network architectures for IDS; no numerical results
[12]	Various well-known datasets	Not specified (focus on preprocessing)	Contribution to preprocessing; no numerical results
[13]	CICIDS 2018	Hybrid DNN + LSTM	F1 99%, PR 99%; high computational cost and longer training time
[14]	N/A (security analysis)	N/A	Discussion of vulnerabilities and attacks on EVs and infrastructure
[15]	Real vehicle tests (CAN bus)	SVM, Decision Tree, Random Forest, MLP	Best: Random Forest — F1 98%, AC 97.2%
[16]	Not specified	VGG16, XBoost	Best: XBoost — F1 98.24%, PR 95.95%
[17]	Not specified	Various, best: XGBoost	Best: XGBoost — F1 99%, PR 99%
[18]	CICEVSE2024	Hybrid CNN-LSTM	AC 97.15%, PR 97.19%, REC 97.15%, F1 97.15%, AUC 97.14%
[19]	CICEVSE2024	Adaptive Random Forest (ARF) + ADWIN	Binary: AC 99.13%, PR 99.99%, REC 99.14%, F1 99.56% Multiclass: AC 98.40%, PR 98.40%, REC 98.40%, F1 98.31%

security of electric vehicle charging stations. Figure 1 illustrates a generic attack scenario on the structure of an electric vehicle, similar to the context where the dataset was generated. This dataset will be used to train the previously mentioned model in III-C. It includes data from attacks carried out on a vehicle and represents these attacks through the CAN BUS protocol. The attacks include *Denial of Service* and *Spoofing* (an attack in which an adversary attempts to impersonate a trusted source to deceive the system) targeting several critical vehicle functions, such as speed and revolutions per minute.

B. Data Preprocessing

The dataset underwent preprocessing using the *MinMax* technique, which is a normalization method that rescales data to a fixed range — in this case, from 0 to 1 — using the *SKlearn*[1] library in the *Python* programming language. Python was chosen for its familiarity and ease of use, as well as its strong community support, extensive libraries, and other important functionalities that simplify the data preprocessing stage.

The training environment used was *Orange Data Mining*, while the code was developed with the *TensorFlow* and *PyTorch* libraries — both open-source machine learning frameworks that provide statistical visualizations, flexibility, and straightforward implementation for most of the code applied in the project.

[1] Available at: https://scikit-learn.org

C. Classification

Several machine learning models were evaluated for the IDS application, considering not only intrusion detection effectiveness but also training time and computational resource consumption. The following supervised classifiers were tested:

- *Random Forest*;
- *Decision Tree*;
- *Naive Bayes*;
- *AdaBoost*;
- *Logistic Regression*;
- *CN2 Rule Induction*;
- Recurrent Neural Networks (*RNN LSTM*).

These machine learning models represent different approaches to classification and regression. The hyperparameters of the tested models were in their default configuration from the implementation library. The Decision Tree creates a flowchart-like model, where each internal node represents a test on an attribute, each branch represents the outcome of the test, and each leaf represents a class label. The *Random Forest* improves upon this by building multiple decision trees during training and outputting the class that is the mode of the classes (classification) or the mean prediction (regression) of

the individual trees. *AdaBoost* (*Adaptive Boosting*) is another ensemble method that sequentially combines multiple weak classifiers (usually one-level decision trees, known as "*decision stumps*"), where each new model corrects the errors of the previous ones. The *CN2 Rule Induction* algorithm learns a set of "if–then" rules directly from the training data, seeking rules that cover a large number of examples with high accuracy.

On the other hand, *Naive Bayes* is a probabilistic classifier based on Bayes' theorem with the "naive" assumption of conditional independence between attributes. Logistic Regression is a linear model that uses a logistic function to model the probability of a given class or event occurring, such as success/failure. Finally, Recurrent Neural Networks (*RNN LSTM*) are a type of artificial neural network designed to recognize patterns in sequential data, such as text or time series. *LSTMs* (*Long Short-Term Memory*) are a specialized RNN architecture designed to learn long-term dependencies, making them highly effective in tasks such as machine translation and speech recognition.

Each model was selected for its specific characteristics and varying computational requirements, enabling a broad comparison between lightweight and more complex algorithms.

The performance evaluation of each model will be based on multiple performance metrics: accuracy (CA), precision (PR), recall (REC), and F1-score (F1), in addition to training time measurements. This set of indicators provides a comprehensive overview of the advantages and limitations of each approach, assisting in the selection of the most suitable model for embedded environments in electric vehicles.

Table II
PERFORMANCE METRICS OF EVALUETED MODELS.

Model	Train (s)	Test (s)	CA	F1	PR	REC
Random Forest	51.801	3.591	0.996	0.996	0.996	0.996
Decision Tree	12.274	0.153	0.975	0.971	0.968	0.975
Naive Bayes	6.905	1.165	0.981	0.981	0.981	0.981
AdaBoost	555.825	23.328	0.996	0.996	0.996	0.996
Logistic Regression	140.490	0.778	0.876	0.842	0.829	0.876
CN2 Rule Induction	936.443	2.374	0.996	0.996	0.997	0.996
RNN LSTM	1125.634	16.708	0.999	0.999	0.999	0.999

IV. RESULTS

This section presents and discusses the results obtained from the implementation of the proposed Intrusion Detection System (IDS). The performance evaluation of the models was conducted using the metrics listed as described in III-C.

The results show that most of the evaluated models achieved satisfactory performance in detecting intrusions in electric vehicles, with high values in the metrics of Accuracy (CA), F1-Score, Precision, and Recall. In particular, the RNN LSTM model achieved the best results, reaching 0.999 in all performance metrics (Accuracy, F1-Score, Precision, and Recall). This high performance comes at the cost of longer training times and, consequently, higher computational demands.

The Random Forest, AdaBoost, and CN2 Rule Induction models also delivered robust performance, with Accuracy, F1-Score, Precision, and Recall values of 0.996. Despite variations in training and testing times, these models demonstrate high detection capability. Among them, it is worth highlighting Random Forest, which achieved similar performance to the others while requiring significantly less training time.

The Naïve Bayes model showed consistent performance, with 0.981 across all performance metrics, and relatively low training and testing times (6.905s and 1.165s, respectively). This makes it a viable option for scenarios where computational efficiency is critical. The Decision Tree model also demonstrated speed (12.274s training, 0.153s testing), with slightly lower—yet still acceptable—performance metrics.

On the other hand, Logistic Regression presented the lowest scores among the evaluated models, with 0.876 for Accuracy and Recall, 0.842 for F1-Score, and 0.829 for Precision. While its testing time was low (0.778s), its detection performance was inferior to the other models.

In summary, the analysis of the results presented in Table II shows that, although the RNN LSTM model achieved the highest scores in all evaluated metrics (CA, F1, PR, and REC = 0.999), its high computational cost, with a training time of 1125.634 s, limits its applicability in embedded environments with energy and processing constraints. Conversely, models such as Random Forest and CN2 Rule Induction achieved very similar performance (CA, F1, PR, and REC = 0.996), but with markedly different training times — 51.801 s for Random Forest and 936.443 s for CN2 Rule Induction — highlighting Random Forest as a more favorable option in terms of accuracy–cost trade-off. The AdaBoost model also produced robust results (CA, F1, PR, and REC = 0.996); however, its high training time (555.825 s) may reduce its attractiveness for scenarios with limited resources. In contrast, Naïve Bayes stood out for its low training (6.905 s) and testing times (1.165 s), with satisfactory performance (CA = 0.981), making it a viable alternative for applications requiring greater computational efficiency. Logistic Regression, on the other hand, presented the lowest overall performance (CA = 0.876), despite a moderate computational cost, indicating lower suitability to the evaluated context. Overall, tree-based models and probabilistic methods show a more favorable cost–benefit ratio for embedded scenarios, whereas deep architectures offer maximum performance at the expense of greater computational consumption.

V. Conclusion

The results obtained demonstrated that most models showed satisfactory performance, with high scores in the metrics of CA, *F1-score*, precision, and *recall*. The *RNN LSTM* model stood out, achieving 0.999 in all performance metrics, proving its effectiveness in intrusion detection, although with higher computational cost and training time. Models such as *Random Forest*, *AdaBoost*, and *CN2 Rule Induction* also exhibited robust performance (0.996 in all metrics), with *Random Forest* standing out due to its shorter training time in comparison. The *Naïve Bayes*, with 0.981 in all metrics and relatively low training and testing times, proved to be a viable option for scenarios with computational constraints. On the other hand, *Logistic Regression* presented the lowest performance among the evaluated models.

Future research could explore the integration of additional deep learning architectures, such as Transformer-based or hybrid models, to further enhance detection accuracy and reduce false positives. It would also be valuable to investigate techniques for model compression, pruning, and quantization, enabling high-performing algorithms like RNN LSTM to operate efficiently in embedded environments with limited computational resources. Moreover, future studies may evaluate the adaptability of these models to new or evolving attack vectors, as well as their performance with real-time streaming data from electric vehicles. Finally, implementing explainability methods and assessing the cybersecurity–energy trade-off would provide a deeper understanding of model behavior and support more reliable deployment in safety-critical automotive contexts.

In summary, the results indicate that the selection of the most appropriate model should consider not only accuracy metrics but also the associated computational costs, particularly in embedded and energy-constrained environments such as those of electric vehicles. Thus, tree-based algorithms and probabilistic methods emerge as more balanced alternatives for practical applications, whereas deep architectures, although superior in performance, require additional optimizations to enable their use in real-world contexts.

Acknowledgments

The authors are grateful to State Center for Technological Education “Paula Souza” (CEETEPS) for research conditions at the Defensive Cybersecurity and Artificial Intelligence Laboratory (Detect.AI), and to Research Support Foundation of São Paulo State (FAPESP), Brazil grants #2023/12830-0.

References

[1] International Energy Agency, “Global ev outlook 2025,” International Energy Agency, Paris, Tech. Rep., 2025. [Online]. Available: https://www.iea.org/reports/global-ev-outlook-2025

[2] D. Ronanki, A. Kelkar, and S. S. Williamson, “Extreme fast charging technology—prospects to enhance sustainable electric transportation,” *Energies*, vol. 12, no. 19, p. 3721, 2019.

[3] J. Caltrider, M. Rykov, and Z. MacDonald, “It’s official: Cars are the worst product category we have ever reviewed for privacy,” *Mozilla Foundation*, 2023.

[4] 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.

[5] S. Soltan, P. Mittal, and H. V. Poor, “BlackIoT:IoT botnet of high wattage devices can disrupt the power grid,” *27th USENIX Security Symposium (USENIX Security 18)*, pp. 15–32, 2018.

[6] Z. Muhammad, Z. Anwar, B. Saleem, and J. Shahid, “Emerging cybersecurity and privacy threats to electric vehicles and their impact on human and environmental sustainability,” *Energies*, vol. 16, no. 3, p. 1113, 2023.

[7] A. Drewek-Ossowicka, M. Pietrołaj, and J. Rumiński, “A survey of neural networks usage for intrusion detection systems,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 497–514, 2021.

[8] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, “Lstm-based intrusion detection system for in-vehicle can bus communications,” *IEEE Access*, vol. 8, pp. 185 489–185 504, 2020.

[9] Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis, and C. Douligeris, “Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (ocpp),” *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1504–1533, 2022.

[10] S. Acharya, Y. Dvorkin, H. Pandžić, and R. Karri, “Cybersecurity of smart electric vehicle charging: A power grid perspective,” *IEEE Access*, vol. 8, pp. 214 434–214 453, 2020.

[11] S. Acharya, Y. Dvorkin, and R. Karri, “Public plug-in electric vehicles + grid data: Is a new cyberattack vector viable?” *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5099–5113, 2020.

[12] X. Larriva-Novo, C. Sánchez-Zas, V. A. Villagrá, M. Vega-Barbas, and D. Rivera, “An approach for the application of a dynamic multi-class classifier for network intrusion detection systems,” *Electronics*, vol. 9, no. 11, p. 1759, 2020.

[13] M. Basnet and M. H. Ali, “Deep learning-based intrusion detection system for electric vehicle charging station,” *2020 2nd International Conference on Smart Power & Internet Energy Systems (SPIES)*, pp. 408–413, 2020.

[14] S. Hamdare, O. Kaiwartya, M. Aljaidi, M. Jugran, Y. Cao, S. Kumar, M. Mahmud, D. Brown, and J. Lloret, “Cybersecurity risk analysis of electric vehicles charging stations,” *Sensors*, vol. 23, no. 15, p. 6716, 2023.

[15] T. Moulahi, S. Zidi, A. Alabdulatif, and M. Atiquzzaman, “Comparative performance evaluation of intrusion detection based on machine learning in in-vehicle controller area network bus,” *IEEE Access*, vol. 9, pp. 99 595–99 605, 2021.

[16] H.-C. Lin, P. Wang, K.-M. Chao, W.-H. Lin, and J.-H. Chen, “Using deep learning networks to identify cyber attacks on intrusion detection for in-vehicle networks,” *Electronics*, vol. 11, no. 14, p. 2180, 2022.

[17] M. A. S. Sardar, H. Saha, M. N. Sultan, and M. F. Rabbi, “Intrusion detection in electric vehicles using machine learning with model explainability,” *J. Inf. Hiding Multim. Signal Process.*, vol. 14, no. 3, pp. 81–89, 2023.

[18] M. M. Rahman, M. M. H. Chayan, K. Mehrin, A. Sultana, and M. M. Hamed, “Explainable deep learning for cyber attack detection in electric vehicle charging stations,” in *Proceedings of the 11th International Conference on Networking, Systems, and Security*, 2024, pp. 1–7.

[19] F. Makhmudov, D. Kilichev, U. Giyosov, and F. Akhmedov, “Online machine learning for intrusion detection in electric vehicle charging systems,” *Mathematics*, vol. 13, no. 5, p. 712, 2025.