Journal of Applied Artificial Intelligence
https://jaai.sabapub.com
ISSN: 2709-5908

2025 Volume 6, Issue 2: 1–14

DOI: https://doi.org/10.48185/jaai.v6i2.1461

Ensemble-based Intrusion Detection System for Electric Vehicles Charging Stations using Machine Learning

Bishal K C[1,*], Kshitiz Aryal[2], Pawan Thapa[3] , Sansrit paudel[4]

[1,2]Department of Computer Science, Tennessee Technological University, Cookeville 38501, USA
[3]Department of Engineering Technology, University of Toledo, Toledo 43606, USA
[4]Department of Computer Science, University of Rhode Island, Kingston 02881, USA

Received: 21.01.2025 • Accepted: 26.11.2025 • Published: 30.12.2025 • Final Version: 31.12.2025

Abstract: Traditional Vehicles have an adverse effect on the environment. Therefore, the current technological shift is constantly seeking an alternative to replace traditional vehicles fueled by fossil fuels, and Electric vehicles are, so far, the best alternative. The adoption of Electric Vehicles (EVs) is growing rapidly due to their eco-friendly benefits and technological advancements. This growth, however, brings a significantly larger attack surface due to increased interconnectivity between electric vehicles, charging stations and the smart grid system. To prevent such types of attacks, we need a robust system to detect them beforehand and prevent the system from being compromised. Although some prior work has been conducted in this area, their approaches did not incorporate deep learning algorithms, nor did they evaluate model performance under noisy data conditions. Therefore, we proposed a novel ensemble-based intrusion detection system (IDS) to detect these attacks in Electric Vehicle Charging Stations (EVCS). We implement different Machine learning algorithms such as k-nearest neighbors (KNN), Logistic Regression (LR), Support Vector Machine (SVM) and Decision Tree (DT). Moreover, as different types of malwares often exhibit distinct structural characteristics when visualized as images, we also use Convolutional Neural Networks (CNNs) to detect such attacks and malware. We are focusing on detecting attacks in Electric vehicle charging stations by analyzing the network traffic. For this, we utilize the latest labelled dataset, the Canadian Institute of Cybersecurity EV Charger Attack Dataset 2024 (CICEVSE2024), which is a multidimensional dataset containing both benign and attack data. We then evaluate & compare the performance of these algorithm in detecting the network traffic attacks in Electric Vehicle Charging Stations (EVCS). Our proposed model employs an ensemble voting strategy to combine the predictions from different classifiers, thereby improving the system's robustness and accuracy, and achieves an accuracy of 99.5% in detecting cyberattacks. With the addition of small noise to the dataset, a few individual classifiers perform poorly; however, the ensemble model still maintains an accuracy of 99.2%.

Keywords: Electric Vehicle (EV), Intrusion Detection System (IDS), Machine Learning (ML), Electric Vehicle Charging Stations (EVCS), Canadian Institute of Cybersecurity EV charger attack dataset 2024 (CICEVSE2024).

[*] Corresponding Author: bkc42@tntech.edu

1. Introduction

Automotive vehicles using fossil fuels have an adverse environmental impact. Therefore, researchers are always searching for alternatives to fossil fuels. In recent years, the worldwide adoption of electric vehicles (EVs) has been growing at a rapid rate. According to a recent U.S. Energy Information Administration (2024) report [1], U.S. combined sales of hybrid vehicles, plug-in hybrid electric vehicles, and battery electric vehicles (BEVs) rose from 17.8% of total new light-duty vehicle sales in the first quarter of 2024 (1Q24) to 18.7% in the second quarter of 2024 (2Q24), according to estimates from Wards Intelligence. [1] As the number of EV sales rises, so does the need to install electric vehicle charging stations. All electric vehicles and charging stations are becoming increasingly digitalized, with an associated risk of data breaches or other security threats. As a result, malicious Internet users are finding new ways to hack charging points and gain access to private user information. It severely concerns the security of EVCS.

EV charging stations are connected to the main grid system, thereby forming a vast network, and the exposure of the attack surface is exponential, presenting numerous possibilities for malicious actors to execute various attacks. Moreover, we face unprecedented risks from cyber-attacks as we move into an era dominated by computerized vehicles, especially electric cars. Vulnerabilities in Electric vehicle chargers can also be exploited by malicious actors to install malware in a charging station. Once the malware is on-site, it can be transferred to an electric vehicle user, potentially disrupting their service in a negative manner. In 2023, a significant increase in large-scale attacks on electric vehicles was reported, approximately 2.5 times more than in 2022, according to Israel-based Upstream [2]. Of these attacks, 95% were carried out remotely, and 85% were long-range attacks done by malicious actors. As these figures indicate, future attacks are expected to become increasingly sophisticated. The main concern for now is to secure the electric vehicle charging station system. Currently, an Intrusion Detection System (IDS) is required to detect a malicious attack before it can damage the system. IDS for EVCS using machine learning, including deep learning, is an emerging and important research area for addressing security vulnerabilities in the growing electric vehicle infrastructure. IDSs based on machine learning and deep learning have already demonstrated effectiveness in detecting various types of attacks due to their ability to identify patterns from large datasets, resulting in enhanced efficiency and accuracy in detecting them.

In this paper, we present the application of various Machine Learning and Deep Learning algorithms to detect malware and malicious attacks on electric vehicle charging stations. Using the publicly available CICEVSE 2024 dataset [3], we use machine learning and deep learning methodologies to detect attacks. We use datasets containing information about network and host attacks on the EV charger in both charging and idle states. Using this dataset, we train and evaluate different machine-learning models that can detect possible malware and malicious attacks. After training individual models, we employ an ensemble voting strategy to combine the predictions from different classifiers, improving the system's robustness and accuracy. We also discuss the performance of various machine learning algorithms and suggest which ones will work most effectively and efficiently. We contribute to developing a more robust and reliable charging infrastructure for electric vehicles by proposing machine learning algorithms to detect cyberattacks on EVCS automatically. The paper is organized as follows: Section 2 introduces the problems in EVCS and describes previous work on the use of ML techniques for detecting malware and malicious attacks, section 3 briefly discusses the datasets used, Section 4 presents the methodology, Section 5 demonstrates the discussion, experimental results and findings of the deployed machine learning and deep learning algorithms and Section 6 concludes the findings and outlines potential future improvements.

2. Background & Related Work

2.1. Background

The common alternatives to traditional vehicles fueled by fossil fuels are electric vehicles. As demand for EVs grows, it opens a vast territory of vulnerability for attackers. Understanding the electric vehicle ecosystem is a crucial starting point before delving deeper into its vulnerabilities. The term EVCS refers to the ecosystem, spanning from power production to smart power grids and EV charging infrastructure, including charging terminals and electric vehicles [4]. The smart or power grid system, charging stations, electric vehicles, and end users are the main components of an EV charging station. The smart power grid integrates digital communication and automation technology to facilitate more efficient electricity generation, distribution, and consumption, as well as dynamic and real-time energy management. Electric vehicles are charged at charging stations, which typically provide various charging speeds and smart features for load balancing and user convenience. An electric motor powers an electric vehicle, where energy is stored in batteries, and end users interact with the charging infrastructure through apps, payment systems, and other interfaces to meet their charging needs. Targeted attackers can target these components of the EVCS ecosystem for malicious purposes. Detailed information about the different types of attacks that can be performed on different components is given below:

Attacks targeting the Smart or Power Grid System: Conventional power grid systems rely on the one-way distribution of power producers to consumers, but smart grid systems leverage the Internet of Things (IoT) to make each node intelligent. With IoT, smart grids become more vulnerable, leaving them with increased attack surfaces for malicious activities. Malicious software or malware infiltrating smart grid systems to cause disruptions is one of the common security threats. Similarly, attackers can eavesdrop on network traffic and gain access to sensitive information or login credentials. Data can also be tampered with when attacked by attackers to cause incorrect energy readings or billing inconsistencies. Moreover, placing excessive traffic on smart grid networks could lead to a Distributed Denial of Service (DDoS) attack, potentially halting operations. In many applications, Electric Vehicles are connected to the grid via V2G communication systems [5], allowing the vehicle to provide power back to the grid. This is a critical point of attack. The attacker can attack V2G to gain access to the power grid itself and disrupt energy distribution or paralyze huge areas with outages. These are some basic attacks that exploiters can perform on the smart grid system.

Attacks on the Electric Vehicle Charging Stations: Electric Vehicle Charging Stations (EVCS) are vulnerable to several attacks: malware injection, man-in-the-middle (MitM) attacks and Denial of Service (DoS) attacks [6]. In particular, attackers can have unauthorized access via EV connectors to infiltrate charging settings or inject malicious code. Through spoofing attacks, they can also compromise the user's identity. Furthermore, unauthorized maintenance terminals and communication ports can be used as listening devices or as devices that alter data. These vulnerabilities not only threaten user safety and privacy but also disrupt the reliability and availability of charging services. Addressing these challenges necessitate strong and well-maintained cybersecurity practices, including data encryption, reliable authentication protocols, and routine security assessments to identify and mitigate potential risks.

Attack Targeting Electric Vehicles and End Users: Data theft and manipulation of onboard systems are also primary attacks targeting electric vehicles and their end users, which often involve remote attacks. Injecting malware into an EV allows malicious actors remote access, as well as the ability to cause system malfunctions, such as rapid battery drain. If EVs are not secure, they can be easily compromised, allowing attackers to steal users' personal data, such as real-time locations, through eavesdropping. This could lead to the risk of identity theft. For example, Tesla Cars, EV charging stations, and even modems and entertainment systems were recently successfully hacked by Synacktiv security researchers at the SPwn2Own event [7]. Similarly, Synacktiv was able to gain access to critical Tesla subsystems in under two minutes via a time-of-check-to-time-of-use (TOCTTOU) attack [8] [9]. In 2022, a cybersecurity expert also hacked into 25 Tesla vehicles spread across 12 countries, took control of critical systems in those vehicles, and exploited the TeslaMate app [10]. In addition, 140,000 users' data was accidentally exposed through a vulnerability in an EV charging app [11]. Clearly, as we can see, these attacks on electric vehicles and the end users are no longer rare; they are becoming common and more sophisticated.

2.2. Related Work

There has been extensive work in identifying vulnerabilities and suggesting several models to further strengthen the electric vehicle ecosystem against such attacks [12-22]. With the increasing availability of computational resources, the incorporation of Artificial Intelligence (AI) into Intrusion Detection Systems (IDS) for Internet of Things (IoT) systems has become more prevalent. Methods such as Logistic Regression (LR), Generative Adversarial Networks (GAN), Decision Trees (DT), and Support Vector Machines (SVM) are used to detect anomalies and malware in networks. In particular, Generative Adversarial Networks (GAN) are very useful for simulating unseen attacks within a system, and they help prevent and detect such attacks in the future. In GANs, models are trained by feeding the data, and the model learns from these datasets. Similarly, Deep Neural Networks (DNN)- based deep learning techniques have also been shown to be effective in intrusion detection systems, achieving high accuracy.

Mohamed et al. [12] proposed a binary classification model and evaluated its accuracy using 124,000 flows, which were distributed between benign and DDoS attack flows. Similarly, the authors in [13] used binary and multi-class classification with 100%, 97.44% and 96.90% accuracy in the binary, six-class and 15-class classifications, respectively. To detect and classify DoS attacks in EVCS, Basnet et al. [14] employed Deep Neural Networks (DNN) and Long Short-Term Memory (LSTM) algorithms, achieving a detection accuracy of more than 99%. Their work revealed that using LSTM is more efficient than using DNN. In [15], Islam et al. proposed an adaptive differential privacy-based federated learning framework and an intelligent privacy allocation mechanism via reinforcement learning. The framework is adaptive to the level of privacy breaching rate and dynamically optimizes the privacy budget and utility without the need for human intervention, such as domain knowledge experts. In the paper [16], the authors experimented with different machine learning algorithms, including Naive Bayes, Support Vector Machines (SVM), and deep learning techniques such as Long Short-Term Memory (LSTM) networks and Deep Neural Networks (DNN) to build an intrusion detection system (IDS) using the Intrusion detection evaluation dataset i.e., CICIDS 2017 dataset. Generative Adversarial Networks (GANs) can also be applied in intrusion detection systems. As highlighted in the survey paper [17], various types of GANs have already been explored for anomaly and malware detection. Moreover, to address the scarcity of cyberattack data, the authors [18] proposed the use of an external classifier Wasserstein condition GAN (EC-WCGAN)-based network intrusion detection system (NIDS) to identify distributed denial-of-service (DDoS) attacks within electric vehicle (EV) charging infrastructures. Al-Mehdhar et al. [19] introduced another hierarchical adversarial framework, HADRL, which utilizes Deep Reinforcement Learning (DRL) and is effective in detecting stealth cyberattacks on EV charging stations, particularly those causing denial of charging. They also developed advanced, stealthy attack methods capable of avoiding basic intrusion detection systems (IDS) using DRL and installed a DRL-based scheme inside the IDS at the EV charging stations to detect and respond to these highly sophisticated attacks. Viboonsang et al. [20] utilized different machine learning models like Random Forest, Decision Tree, Logistic Regression and K-Nearest Neighbors (KNN) and deep learning models like Recurrent Neural Network (RNN) to categorize the NSL-KDD dataset into either attack or normal traffic. Kondu et al. [21] similarly propose an anomaly detection model in EVC systems through deep learning approaches i.e. Long Short-term Memory (LSTM) with a 99.589% accuracy. Similarly, Hussain et al. [22] suggested data-driven anomaly detection (DDAD) techniques by leveraging a Bi-directional Long Short-Term Memory (Bi-LSTM) network to secure electric vehicle charging stations (EVCS) in a Hardware-in-the-Loop (HIL) iCPS testbed of a DER-integrated EVCS microgrid model. They used real time cyber-attacks such as denial-of-service (DoS) attacks, spoofing, replay, and data manipulation attacks in the microgrid based EVCS test system to demonstrate an accuracy of 99.42%.

According to the literature above, machine learning methods and deep learning techniques are effective in detecting malicious attacks in networks, and thus these methods can alert systems to such behaviors, acting as an Intrusion Detection System (IDS). Additionally, Generative Adversarial Networks (GANs) can help solve the issue of insufficient cyber-attack data by generating new cyber-attack datasets. Although the above-proposed methodology has impressive accuracy, they are trained on very limited or generated datasets. Therefore, our research will focus on the latest published dataset, namely the CICEVSE 2024 dataset [3], and evaluate the performance of different algorithms in detecting attacks in EVCS. We are not only evaluating different classifiers, but we are also using the predictions from the various models to make the final prediction. We are implementing the stacking ensemble technique to increase the accuracy & robustness of the model. In brief, we proposed an ensemble model that aggregates the predictions of multiple models through voting to enhance accuracy and robustness. To further evaluate the model's resilience, we introduce controlled noise into the dataset and analyze its performance under these conditions.

3. Dataset

For our experiment, we utilized the latest published open-source dataset, specifically the CIC EV Charger Attack Dataset 2024 (CICEVSE2024) [3], which was developed by a researcher at the Canadian Institute of Cybersecurity. This dataset is a multi-dimensional labelled dataset containing benign and attack scenarios. The attack-labeled dataset comprises network and host attacks on the Electric Vehicle Supply Equipment (EVSE) charger in both idle and charging states. Moreover, Network attacks consist of various Reconnaissance and Denial-of-Service (DoS) attacks, while host attacks include backdoors and cryptojacking. The testbed setup consists of an operational Level 2 charging station (EVSE-A), a Raspberry Pi, and communication equipment. Raspberry Pi are used for the Electric Vehicle Communication Controller (EVCC), another charging station (EVSE-B), a Power Monitor, and the local Charging Station Monitoring System (CSMS). EVSE-A communicates with a remote CSMS via the OCPP protocol, while EVSE-B interacts with the EVCC using ISO 15118 and the local CSMS via OCPP [23]. Additionally, the power consumption of EVSE-B is tracked by a Raspberry Pi using a wattmeter and I2C protocol. We are constantly looking for the latest EV charging attack dataset for our research, and this dataset perfectly meets our search criteria as it comprises power consumption data, network traffic, and host activities of the EVSE in both benign and attack conditions. For our experiment, we utilized HPC and kernel events from the EVSE-B dataset to train our model to detect attacks in the network system.

4. Methodology

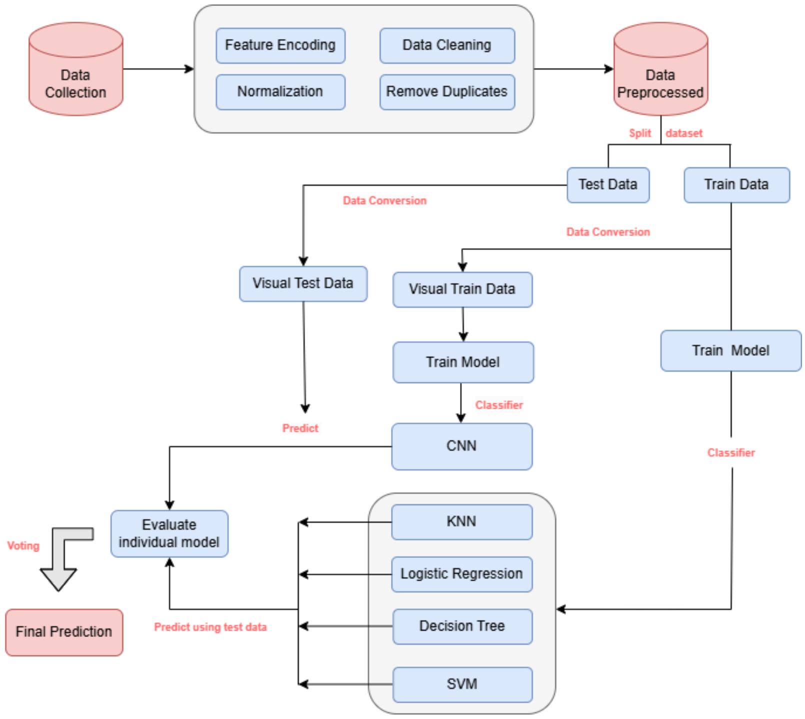

Figure 1. Proposed Ensemble Model Flow diagram

```
Algorithm 1: Ensemble-Based Intrusion Detection System
  Input: Pre-collected dataset with features and labels
  Output: Final prediction using an ensemble-based model
Initialize set of trained models $T \leftarrow \emptyset$;
Preprocess the dataset: encoding, normalization, and cleaning;
Split the dataset into training and testing subsets;
Convert data into a format compatible with ML models;
Define the list of models: CNN, KNN, Logistic Regression, Decision Tree, SVM;
foreach model in the list of models do
    Train the model on the training data;
    Evaluate the model on the testing data;
    Add the model's predictions to $T$;
Combine predictions from all models in $T$ using a voting mechanism;
Generate the final prediction based on the combined votes;
return Final Prediction;
```

The workflow of our proposed model is shown in Figure 1 along with the algorithm that we implemented. Various data processing steps are applied after data collection before training different machine learning models. The duplicated features were identified in the dataset and eliminated them. Feature encoding was performed to transform categorical data into numerical values. Since most of the features were numerical and only a few were categorical, we identified the categorical features and employed One-Hot Encoding for those without any inherent order or ranking, as well as Label Encoding for those with ordinal data. The data was symmetrically distributed and the missing values were handled by using mean imputation. To ensure that each feature contributes equally, we also normalized or scaled the dataset to an appropriate scale. After these preprocessing steps, the dataset was ready for model training. We then split the dataset into training and testing datasets. Furthermore, we also utilize Convolutional Neural Networks (CNNS), which are specifically designed to process image-based input. For that, we transform the structured (tabular) data into visual representations. This transformation is particularly beneficial in the context of malware analysis where encoding structured features or binary representations into grayscale images allows identifying visual patterns. Different types of malwares often exhibit distinct structural characteristics when visualized as images, which may not be as apparent in raw tabular form. By introducing a spatial structure to the data, this transformation enables CNNs to effectively extract and learn hierarchical features, thereby enhancing the model's ability to distinguish between various malware classes. This approach leverages the strengths of CNNs in spatial feature extraction, contributing to improved detection performance. The dataset we used for our experiments was labelled, so we used supervised learning techniques. We applied k-Nearest Neighbours (KNN), Logistic Regression (LR), Support Vector Machine (SVM), and Decision Tree (DT) algorithms, and for deep learning algorithms, we used Convolutional Neural Network (CNN) to identify the underlying attack patterns. After training each model, we evaluated its performance using various performance metrics. We then applied an ensemble technique to aggregate the predictions of each model using voting with and without a noisy dataset and compared the accuracy. For our experimental purpose, we used Python programming language along with the libraries such as Pandas, Numpy, Seaborn, Matplotlib, Scikit-learn, Tensorflow, and Keras. These libraries helped with data handling, preprocessing, machine learning, deep learning, and model evaluation. Additional tools, such as itertools, tabulate, and termcolor, were used for utility and formatting purposes. From our experiments, we found that the accuracy of the model can be improved significantly using an ensemble model.

5. Discussion & Experimental Results

5.1. Experimental Setup

Different machine learning and deep learning methods were used to detect attacks in EVCS. These include Logistic Regression (LR), K-Nearest Neighbors (KNN), Decision Tree (DT), Support Vector Machine (SVM), and Convolutional Neural Network (CNN). These models were chosen for their varied strengths in classification tasks. Logistic Regression (LR) is used for binary classification problems. It estimates the probability that a given input belongs to a particular class by applying the logistic (sigmoid) function. The output is a probability, which is converted into a class label based on a decision threshold. K-Nearest Neighbor (KNN) is a non-parametric algorithm that classifies data points based on the majority class of their nearest neighbors, making it practical for small, well-labeled datasets. Decision Trees (DTs) provide a transparent model by using a tree-like structure to split data based on feature importance, making it easy to interpret. Support Vector Machine (SVM) excels in finding an optimal hyperplane to separate data into distinct classes, mainly when the dataset is linearly separable. Lastly, Convolutional Neural Network (CNN) leverages its strength in deep learning to automatically extract features from data and learn complex patterns, making it well-suited for more sophisticated attack detection tasks.

The experiment was conducted using a machine with the Windows 11 Enterprise 64-bit operating system. The processor was an 11th Gen Intel® Core™ i7-11700 @ 2.50 GHz with 8 cores. The system used have 16 GB of RAM and the graphics card used was an NVIDIA GeForce GTX 1650 with 4 GB of dedicated GPU memory and support for DirectX 12 (FL 12.1). The tool used to run the experiment was Anaconda Jupyter Notebook. All these hardware and software configurations are given in Table 1.

Table 1. Hardware and software specifications used in the experiment.

Component	**Specification**
Operating System	Windows 11 Enterprise 64-bit, Version 22H2, Build 22621.4890
Processor	11th Gen Intel® Core™ i7-11700 @ 2.50 GHz (8 Cores)
Memory	16 GB DDR4
Graphics Card	NVIDIA GeForce GTX 1650, 4 GB Dedicated Memory, DirectX 12 (FL 12.1)
Software	Anaconda Jupyter Notebook

5.2. Performance Metrics

To detect the attacks in the EVCS, we train our models using a labeled dataset and evaluate their performance by calculating accuracy, precision, recall, and F1 score for each of the algorithm. These statistics are universally acknowledged and are popularly used for evaluation purposes. Moreover, the metrics involved include the Confusion Matrix, Classification Accuracy, Precision, Recall, F1 Score, True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). True Positive refers to the number of attack samples correctly identified as attack samples. True Negative refers to the number of benign samples correctly detected as benign samples. False Positive is determined by the number of benign samples incorrectly identified as attack samples, while False Negative represents the number of attack samples incorrectly identified as benign samples.

We evaluated the performance of different models using the above mentioned metrics and as given below:

5.2.1 Accuracy

The accuracy of a model is simply measured by comparing the test samples that are correctly identified with a total number of test samples. The accuracy of the model is given by:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \tag{1}$$

5.2.2 Precision

The precision of a model is calculated by comparing the number of correctly identified attack samples to the total predicted as attack. It measures the model's accuracy in classifying instances as attack and emphasizes its ability to minimize misclassifications as attack.

$$\text{Precision} = \frac{TP}{TP+FP} \tag{2}$$

5.2.3 Recall

The Recall (True Positive Rate or Sensitivity) represents the ratio of accurately detected attack samples to the total number of actual attack samples. It evaluates the model's ability to detect all actual attack instances.

$$\text{Recall} = \frac{TP}{TP+FN} \tag{3}$$

5.2.4 F1 Score

F1 score is the harmonic mean of precision and recall; it serves as a composite metric that captures the fundamental balance between precision and recall. The unified evaluation of the model's overall performance is provided by it, which is given by,

$$\text{F1 Score} = 2 * \left(\frac{Precison*Recall}{Precision+Recall}\right) \tag{4}$$

We trained our models and used the above performance metrics to evaluate each of them.

5.3. Critical Analysis & Results

The use of ensemble techniques is not new in the field of machine learning. Numerous studies have already explored such techniques to enhance performance across various domains. However, best of our knowledge, most existing works have focused only on individual machine learning or deep learning algorithms for detecting attacks in electric vehicle charging stations. Miskin et al. [16] proposed an intrusion detection system (IDS) for EVCS using machine learning models such as Naive Bayes and Support Vector Machine (SVM), along with deep learning models like Deep Neural Networks (DNN) and Long Short-Term Memory (LSTM). Among these, LSTM achieved the highest accuracy of 99.98%. However, they did not explore ensemble or hybrid approaches, which would have limited adaptability to evolving threats. Similarly, ElKashlan et al. [12] also proposed a machine learning-based intrusion detection system (IDS) for electric vehicle charging stations using classical classifiers such as Naïve Bayes, J48 (C4.5 decision tree), Attribute Selection, and a Filtered Classifier. Filtered Classifier worked best with a 99.2% accuracy in both settings. However, they did not go further into deep learning models or ensemble learning techniques, which can have greater flexibility and robustness in variable settings. Therefore, our proposed model differs from their approaches, as we combine both machine learning and deep learning techniques to improve intrusion detection capabilities. Unlike previous work, we study hybrid models that can dynamically adapt to evolving cyber-attacks. We also leverage the use of Convolutional Neural Networks (CNNs) typically employed in image processing by transforming malware traffic data into grayscale images. This transformation gives malware data a spatial characteristic which enables CNNs to detect distinctive structural patterns and hierarchical features less obvious in their original tabular form. Consequently, our approach enhances the model’s ability to accurately detect malware, particularly novel or obfuscated cyberattacks. Experimental results further validate the efficacy of our proposed model, achieving an overall accuracy of 99.5%. Notably, the model demonstrates robustness under challenging conditions, maintaining an accuracy of 99.2% even when subjected to noisy data inputs. This highlights the model's resilience and suitability for deployment in real-world scenarios characterized by data variability and perturbations.

Our first experimental results are shown in Table 2. From the table, it is evident that the ensemble model's accuracy is not significantly improved compared to individual models; however, it does enhance the detection accuracy to some extent and can be utilized as an intrusion detection system. The ensemble model not only improves accuracy but also provides robustness. As we can see even if two of the models perform poorly, the remaining three models can still detect the attack demonstrating the model's flexibility in detection. As demonstrated in Table 2, the ensemble model achieves the highest F1 score and precision, indicating its superior ability to balance recall and precision. This makes the ensemble model particularly effective in minimizing false positives while maintaining high detection rates. Such robustness ensures its suitability for real-world applications where consistent and accurate intrusion detection is critical.

Table 2. Performance of different ML algorithms

Algorithm	Precision	Recall	F1 Score	Accuracy
LR	1	0.98	0.99	98.5%
KNN	0.996	0.991	0.993	99.1%
DT	0.983	0.993	0.988	98.3%
SVM	0.984	0.992	0.987	99.2%
CNN	0.996	0.989	0.992	98.9%
Ensemble	1	0.995	0.997	99.5%

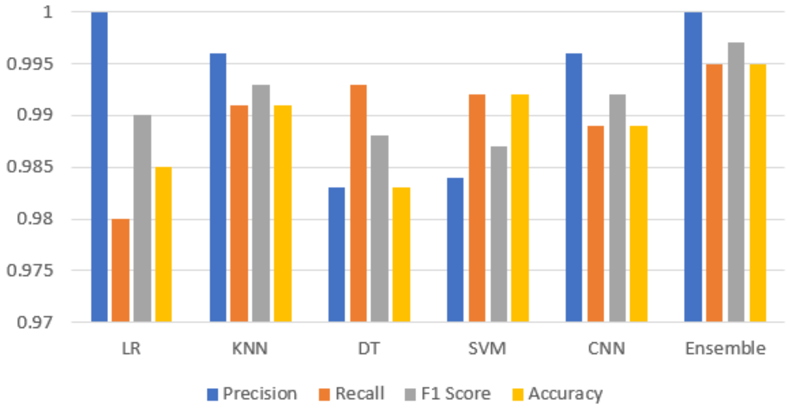

Figure 2. Performance of the classifiers to detect attack

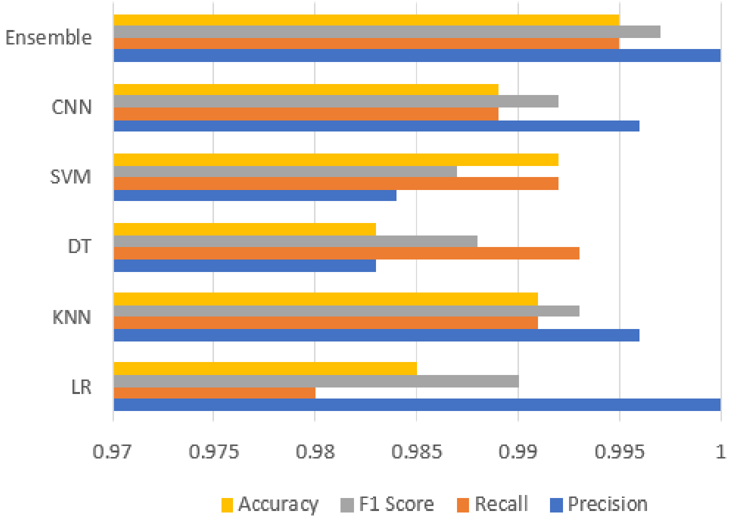

Figure 3. Performance of the classifiers to detect attacks

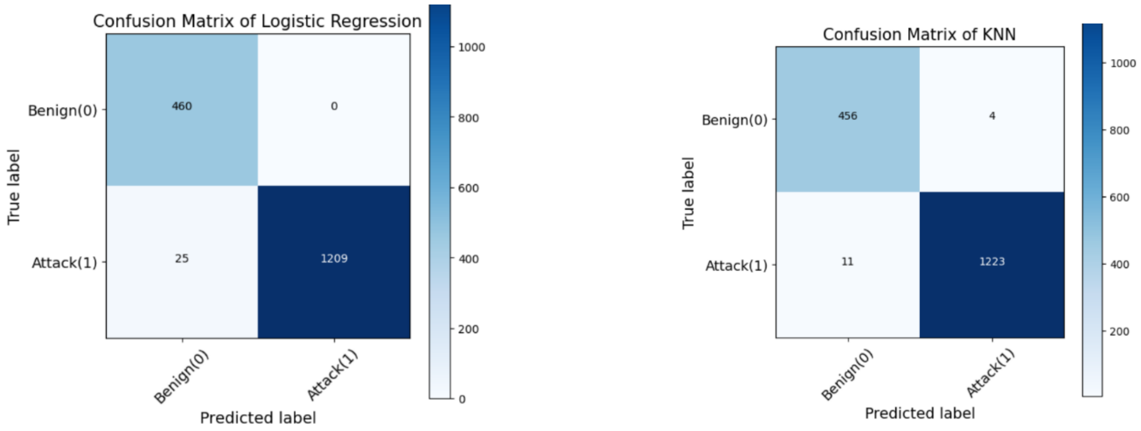

Figure 4. Confusion Matrix for Logistic Regression & KNN

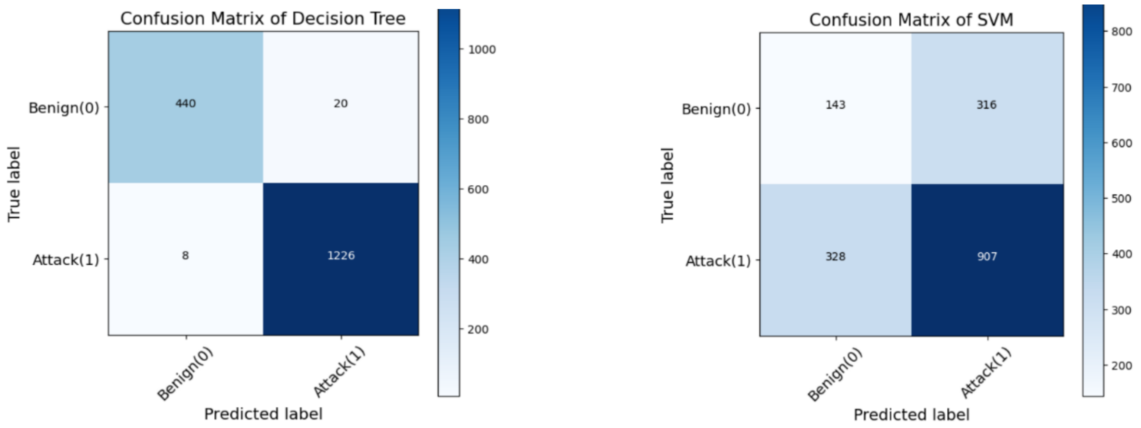

Figure 5. Confusion Matrix for Decision Tree & SVM

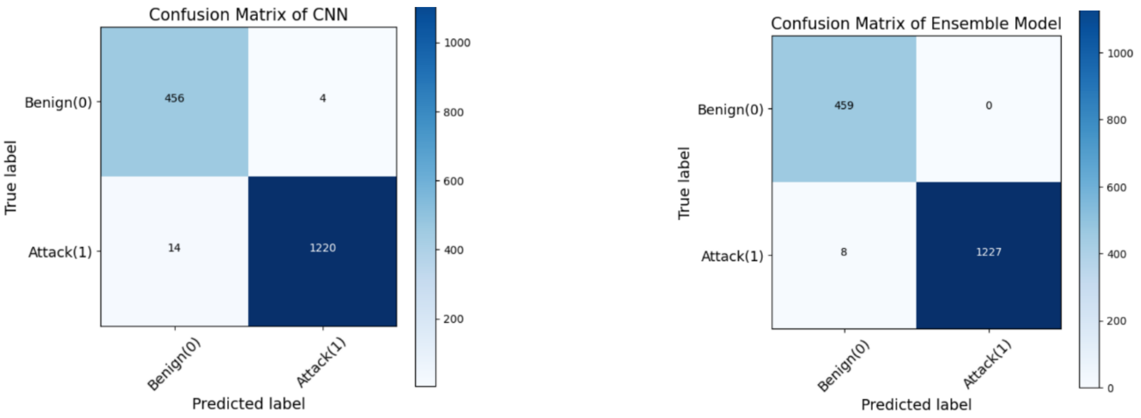

Figure 6. Confusion Matrix for CNN & Ensemble Model

The performance of the different classifiers is illustrated in Figures 2 and 3. These figures shows that the ensemble model performs better than all the other individual models, showing its better ability to aggregate information from multiple models for better prediction. The same is shown in Figures 4 through 6, which show the confusion matrices for all of the models, enabling us to plot the number of right and wrong predictions for each class. In Figure 6, we can observe a total of 8 incorrect predictions, which evidently represents the high reliability and accuracy of the ensemble model. The confusion matrices in Figures 4 to 6 also present the strengths and weaknesses of individual models. For instance, there are more false positives and there are other models that are weak in the ability to handle false negatives. The ensemble model minimizes these flaws by performing collective predictions, hence resulting in improved overall performance. Additionally, we modified the label dataset and some of its columns to introduce noise into the dataset. After that, we conducted another experiment by introducing noise into the dataset, and the results of this experiment are presented in Table 3 below, demonstrating the impact of data perturbations on the model's performance.

Table 3. Performance of different ML algorithms when adding noise

Algorithm	Precision	Recall	F1 Score	Accuracy
LR	0.999	0.755	0.860	82.17%
KNN	0.995	0.991	0.993	99.10%
DT	0.981	0.989	0.986	98.10%
SVM	0.982	0.989	0.981	99.00%
CNN	0.999	0.993	0.992	98.80%
Ensemble	1	0.989	0.994	99.20%

Our second experiment involved the addition of distortions to the data. The accuracy of Logistic Regression model shows an enormous drop with accuracy decreasing from 98.5% to 82.17%. This decrease in accuracy clearly shows that the model is data perturbation sensitive and therefore not as reliable when given noisy or modified data. As opposed to this, the ensemble model was still robust enough to have a high accuracy of 99.2% that shows their robustness along with capacity for dealing with data perturbations extremely well. The ensemble approach, which leverages multiple individual models, proved to be more resilient to these changes in the dataset, maintaining strong performance even under conditions where noise was introduced. This highlights the advantage of using an ensemble model for enhanced stability and accuracy in situations involving imperfect or noisy data. This finding emphasizes the importance of ensemble models in handling imperfect datasets, as they reduce the dependency on a single model's performance. While individual models like Logistic Regression exhibited a significant drop in accuracy when noise was introduced, the ensemble model demonstrated its ability to maintain high performance and reliability. This robustness under noisy conditions reinforces the ensemble model's suitability for real-world applications, where data imperfections are often unavoidable. So, these findings demonstrate that integrating multiple models not only enhances detection accuracy but also contributes to more excellent stability in dynamic and potentially noisy environments.

6. Conclusion

This research aims to detect intrusions and attacks on electric vehicle charging stations through the use of ensemble techniques that combine the predictions of multiple machine learning and deep learning algorithms. Our proposed approach integrates data preprocessing techniques such as feature encoding, data cleaning, normalization of the data, and duplicate removal, in addition to combining the predictions of different models through voting. Additionally, we tested our model with data perturbations, and it maintained high accuracy. Even when one model performed poorly, the other models were still able to detect the attacks. The ensemble model outperforms other algorithms in terms of accuracy, precision, recall, and F1 score. For our experiment, we use stacking techniques to demonstrate the potential of an ensemble model. Future directions could involve implementing boosting techniques, such as AdaBoost and Gradient Boosting, to further enhance the performance of the ensemble model by focusing on instances that are difficult to classify. In addition, use of the hybrid ensemble approaches that combine stacking, boosting and bagging, could also provide further improvements in accuracy and robustness. In summary, our research contributes to the development of an ensemble-based IDS, providing a valuable tool for domain experts and researchers in the field of cybersecurity for electric vehicle charging stations. By building upon the methodologies and results presented in this study, future research can pave the way for more advanced and reliable intrusion detection systems, ensuring the safety and security of EV charging infrastructure.

Acknowledgment

The main scope and purpose of this research, including the conceptual investigations and manuscript preparation, were solely undertaken by the authors. All datasets, tools, models, and sources utilized for the execution of this research have been properly retrieved, cited, and acknowledged where relevant.

References

[1] M. Abboud, "U.S. Energy Information Adminstration," Wards Intelligence, 26 August 2024. [Online]. Available: https://www.eia.gov/todayinenergy/detail.php?id=62924.

[2] "From Experimental to Massive-Scale Attacks," Upstream, 2024. [Online]. Available: https://upstream.auto/reports/global-automotive-cybersecurity-report/.

[3] E. D. Buedi, A. A. Ghorbani and . S. Dad, "Enhancing EV Charging Station Security Using A Multi-dimensional Dataset : CICEVSE2024," in *ESORICS 2024 Conference*, 2024.

[4] L. Zorko, "EV Charging Ecosystem: Explaining the big picture behind it," Tridens Technology, 3 April 2023. [Online]. Available: https://tridenstechnology.com/ev-charging-ecosystem/.

[5] M. S. Mastoi, S. Zhuang, H. M. Munir, M. Haris, M. Hassan, M. Alqarni and B. Alamri, "A study of charging-dispatch strategies and vehicle-to-grid technologies for electric vehicles in distribution networks," *Energy Reports,* vol. 9, pp. 1777-1806, 2023.

[6] 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, 2023.

[7] G. Baran, "Researchers Uncovered 24 Zero-days in Pwn2Own Automotive : Day 1," Cyber Security News, 24 January 2024. [Online]. Available: https://cybersecuritynews.com/pwn2own-automotive-2024-day-1/.

[8] J. Vijayan, "Tesla Model 3 Hacked in Less Than 2 Minutes at Pwn2Own Contest," Dark Reading, 15 March 2023. [Online]. Available: https://www.darkreading.com/vulnerabilities-threats/tesla-model-3-hacked-2-minutes-pwn2own-contest.

[9] J. Wei and C. Pu, "TOCTTOU Vulnerabilities in UNIX-Style File Systems: An Anatomical Study," in *4th USENIX Conference on File and Storage Technologies (FAST 05)*, USENIX Association, 2005.

[10] D. Colombo, "How I got access to 25+ Tesla's around the world. By accident. And curiosity.," Medium, 24 January 2022. [Online]. Available: https://medium.com/@david_colombo/how-i-got-access-to-25-teslas-around-the-world-by-accident-and-curiosity-8b9ef040a028.

[11] A. Laughlin, "Pod Point electric car chargers: security flaw may have put 140,000 app users' data at risk," Which?, 4 November 2021. [Online]. Available: https://www.which.co.uk/news/article/pod-point-electric-car-chargers-security-flaw-may-have-put-140000-app-users-data-at-risk-auIw98m8nI0u.

[12] M. ElKashlan, H. Aslan, M. S. Elsayed, A. D. Jurcut and M. A. Azer, "Intrusion Detection for Electric Vehicle Charging Systems (EVCS)," *Algorithms,* vol. 16, no. 2, p. 75, 2023.

[13] D. Kilichev, D. Turimov and W. Kim, "Next–Generation Intrusion Detection for IoT EVCS: Integrating CNN, LSTM, and GRU Models," *Mathematics,* vol. 12, no. 4, p. 571, 2024.

[14] M. Basnet and M. Hasan Ali, "Deep Learning-based Intrusion Detection System for Electric Vehicle Charging Station," in *2020 2nd International Conference on Smart Power & Internet Energy Systems (SPIES)*, 2020.

[15] S. Islam, S. Badsha, S. Sengupta, I. Khalil and M. Atiquzzaman, "An Intelligent Privacy Preservation Scheme for EV Charging Infrastructure," *IEEE Transactions on Industrial Informatics,* vol. 19, no. 2, pp. 1238-1247, 2023.

[16] S. Vinod Miskin, P. Chandaragi and U. V Wali, "Intrusion Detection System for Electric Vehicle Charging Station," in *2023 3rd International Conference on Mobile Networks and Wireless Communications (ICMNWC)*, 2023, pp. 1-7.

[17] B. K C, S. Sapkota and A. Ashish, "Generative Adversarial Networks in Anomaly Detection and Malware Detection: A Comprehensive Survey," *Advances in Artificial Intelligence Research,* vol. 4, no. 1, p. 18–35, 2024.

[18] M. Basnet and M. H. Ali, "WCGAN-Based Cyber-Attacks Detection System in the EV Charging Infrastructure," in *2022 4th International Conference on Smart Power & Internet Energy Systems (SPIES)*, 2022, pp. 1761-1766.

[19] M. Al-Mehdhar, A. Albaseer, M. Abdallah and A. Al-Fuqaha, "Charging Ahead: A Hierarchical Adversarial Framework for Counteracting Advanced Cyber Threats in EV Charging Stations," in *2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring)*, 2024, pp. 1-6.

[20] P. Viboonsang and S. Kosolsombat, "Network Intrusion Detection System Using Machine Learning and Deep Learning," in *2024 IEEE International Conference on Cybernetics and Innovations (ICCI)*, 2024, pp. 1-6.

[21] V. Kondu and S. Chandana, "Machine Learning and Deep Learning-Based Anomaly Detection for Electric Vehicle Charging Infrastructure and Industrial Internet of Things," *Iowa State University ProQuest Dissertations & Theses,* 2024.

[22] A. Hussain, A. Yadav and G. Ravikumar, "Anomaly Detection using Bi-Directional Long Short-Term Memory Networks for Cyber-Physical Electric Vehicle Charging Stations," *IEEE Transactions on Industrial Cyber-Physical Systems,* pp. 1-11, 2024.

[23] "CIC EV charger attack dataset 2024 (CICEVSE2024)," Canadian Institute of Cybersecurity, 2024. [Online]. Available: https://www.unb.ca/cic/datasets/evse-dataset-2024.html. [Accessed 08 September 2024].