algorithms

MDPI

Article

Intrusion Detection for Electric Vehicle Charging Systems (EVCS)

Mohamed ElKashlan [1], Heba Aslan [1], Mahmoud Said Elsayed [2,*], Anca D. Jurcut [2] and Marianne A. Azer [1,3]

[1] School of Information Technology and Computer Science, Nile University, Cairo 12677, Egypt
[2] School of Computer Science, University College Dublin, Belfield, Dublin 4, Ireland
[3] National Telecommunication Institute, Nile University, Cairo 4433260, Egypt
* Correspondence: mahmoud.abdallah@ucdconnect.ie

Abstract: The market for Electric Vehicles (EVs) has expanded tremendously as seen in the recent Conference of the Parties 27 (COP27) held at Sharm El Sheikh, Egypt in November 2022. This needs the creation of an ecosystem that is user-friendly and secure. Internet-connected Electric Vehicle Charging Stations (EVCSs) provide a rich user experience and add-on services. Eventually, the EVCSs are connected to a management system, which is the Electric Vehicle Charging Station Management System (EVCSMS). Attacking the EVCS ecosystem remotely via cyberattacks is rising at the same rate as physical attacks and vandalism happening on the physical EVCSs. The cyberattack is more severe than the physical attack as it may affect thousands of EVCSs at the same time. Intrusion Detection is vital in defending against diverse types of attacks and unauthorized activities. Fundamentally, the Intrusion Detection System's (IDS) problem is a classification problem. The IDS tries to determine if each traffic stream is legitimate or malicious, that is, binary classification. Furthermore, the IDS can identify the type of malicious traffic, which is called multiclass classification. In this paper, we address IoT security issues in EVCS by using different machine learning techniques and using the native IoT dataset to discover fraudulent traffic in EVCSs, which has not been performed in any previous research. We also compare different machine learning classifier algorithms for detecting Distributed Denial of Service (DDoS) attacks in the EVCS network environment. A typical Internet of Things (IoT) dataset obtained from actual IoT traffic is used in the paper. We compare classification algorithms that are placed in line with the traffic and contain DDoS attacks targeting the EVCS network. The results obtained from this research improve the stability of the EVCS system and significantly reduce the number of cyberattacks that could disrupt the daily life activities associated with the EVCS ecosystem.

Keywords: DDoS; electric vehicle charging stations; EVCS; intrusion detection; Internet of Things (IoT); machine learning; security

Citation: ElKashlan, M.; Aslan, H.; Said Elsayed, M.; Jurcut, A.D.; Azer, M.A. Intrusion Detection for Electric Vehicle Charging Systems (EVCS). *Algorithms* **2023**, *16*, 75. https://doi.org/10.3390/a16020075

Academic Editor: Arun Kumar Sangaiah

Received: 5 December 2022
Revised: 25 January 2023
Accepted: 28 January 2023
Published: 31 January 2023

1. Introduction

EV charging stations have become popular in smart cities. Different countries want to adopt EVCSs quickly [1,2]. These new charging stations use IoT to make life easier and allow EVCS operators more control. As an IoT device, the EVCS is always online to expand client services. This opens the door to cyberattacks on the EVCS ecosystem. The EVCSs are not only affected by the attacks but also both the electrical grid's infrastructure and customers equally. Customers, Electric Vehicle Charging Stations (EVCSs), and the Electricity Grid make up the EVCS Ecosystem, as shown in Figure 1. All the EVCS ecosystem components are vulnerable to IoT cyberattacks [3]. While the long-term EVCS expansion needs rapid infrastructure development, this requires reliable electric vehicle charging stations. It is worth mentioning that there are a set of protocols that govern communication within the EVCS ecosystem. The Open Charge Point Protocol (OCPP) is a communication protocol for

electric vehicle charging stations. It allows for the remote monitoring and management of the charging process, as well as the collection of usage data.

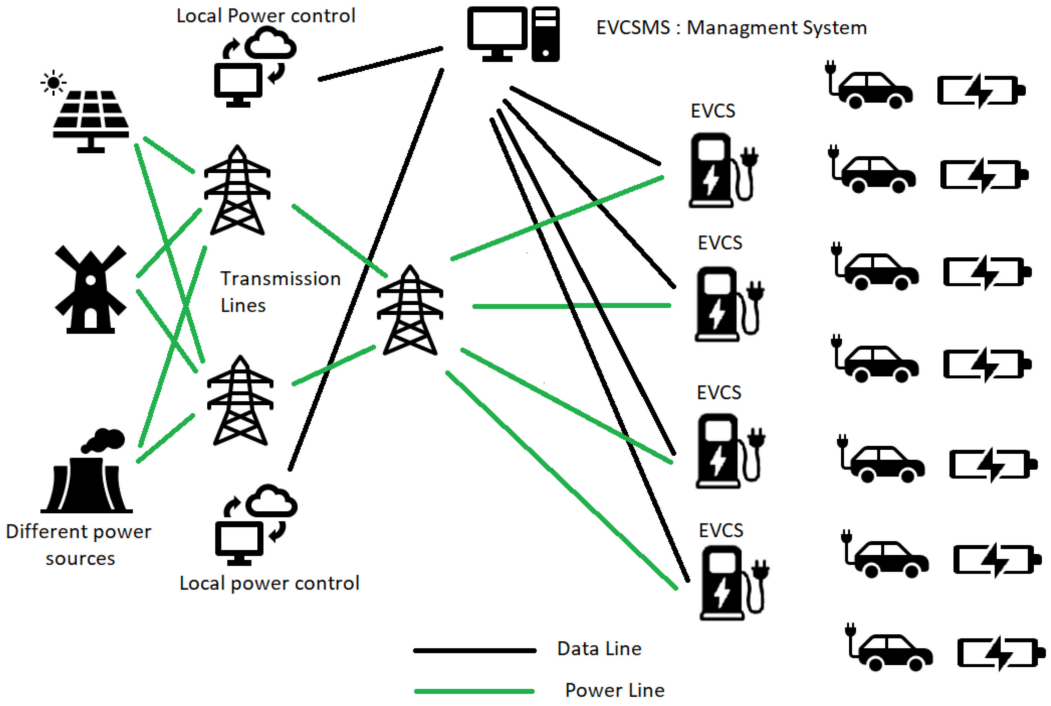

Figure 1. EVCS components forming the EVCS Ecosystem.

ISO 15118 is a set of international standards for communication between electric vehicles and charging stations. It defines the protocols and procedures for secure and efficient charging and payment transactions. Likewise, ISO/SAE 21434 is a standard for the cybersecurity of road vehicles. It provides guidelines for the design and development of secure systems, networks, and components in vehicles, including electric vehicles and charging stations. It is intended to help protect vehicles against cyber-attacks and ensure the safety and security of passengers and other road users.

The IoT ecosystem enriches the EVCS charging station with data. The IoT converts the dummy EVCS stations into an intelligent system that can facilitate the usage and control of these EVCS. This is achieved by enriching the EVCS with data through the IoT. This allows software developers to offer remote monitoring and user accounting to end users. The users can remotely schedule EV charging based on night-time electricity costs. However, this comes with extra challenges. The EVCS equipped with IoT technology became a target for the attackers. There are different techniques in the IT world to detect malicious traffic, such as the Intrusion detection system. However, sophisticated attackers' techniques for staying undetected by IDS, while sending malicious messages through the IoT system, make it difficult to distinguish between malicious and legitimate traffic. IoT network security trumps IT network security. The continual connection needed to serve clients and the large amount of data sent between nodes are the main causes [4]. There are continuous efforts to enhance the effectiveness and accuracy of Intrusion Detection Systems (IDSs), which monitor network traffic to identify potentially harmful data exchanges in IT and IoT environments. To accurately assess IDS systems, it is necessary to use appropriate data [5]. Machine Learning (ML) and Deep Learning (DL) algorithms speed up the development of IDSs that can identify cyberattacks more quickly and accurately [6] making intrusion detection a prominent issue in academics. Costs associated with data breaches in the energy industry have skyrocketed, according to recent research [7].

There is a clear gap in the research for securing the EVCS systems. That is why in this research we focus on the proposed methods to secure the EVCS ecosystem using a

machine-learning-based Intrusion detection system to be used in anomaly detection with high accuracy and low false-positive rates. There are little to no proposals to secure the EVCS ecosystem. This paper defines the EV charging environment, EVCS, communication and transport protocol, and EVCSMS management system. Each component's biggest dangers, in addition to attack vectors and ecosystem weaknesses, are presented. This includes charging station, user, and power grid attacks. In the context of this research, we deal with the IoT component of the EVCS. Therefore, throughout this paper, the terms EVCS and IoT are used interchangeably to denote the IoT component of the EVCS. We apply different Machine learning classifying algorithms with an IoT dataset to examine the IDS response and accuracy in the EVCS ecosystem. We also compare two dominant classifying techniques in defending EVCSs against DDoS attacks.

The following are the paper's contributions:

1. Using a native IoT dataset and different Machine Learning classifying techniques to discover fraudulent traffic in EVCSs.
2. Identifying malicious traffic using a limited number of training data, which increases the agility of the system.

The remaining sections are structured, as follows: Section 2 discusses the background of the EVCS and the associated attacks. In Section 3, we present the work performed in the literature to secure IoT systems with ML and DL-based IDSs. Section 4 describes the methodology and components utilized to simulate the real scenario of traffic flowing in the EVCS/IoT system. Section 5 contains the experimental findings that illustrate the outcomes of various Machine Learning classifier algorithms. Section 6 contains the discussion and limitations of this study. Then the paper is concluded in Section 7 along with future work.

2. Background

Since the EVCS system is still developing, it presents a sizable target for malicious actors. This makes it an easy target for adversaries, whether state-sponsored or not. Public and private EVCSs are both at risk since more of these systems are connected to the Internet and hence more vulnerable to attack. Exploitation may occur remotely over the Internet or locally on a Local Area Network (LAN) if the EVCS network's access is through LAN.

The Internet of Things (IoT) and Electric Vehicle Charging Stations (EVCS) are linked using communication protocols and technologies that allow for remote monitoring, management, and control of the charging process. IoT technologies such as sensors, wireless communication, and cloud computing are used in EVCS to provide real-time data on charging status, energy consumption, and other relevant information. These data can be used to optimize the charging process and improve the overall efficiency of the EVCS.

Additionally, IoT technologies can be used to connect EVCS to other systems, such as smart grid infrastructure and payment systems, allowing for seamless integration and automation of charging and payment transactions. The use of IoT technologies in EVCS also enables remote monitoring and management of the charging process, allowing for the detection and resolution of issues, as well as the collection of usage data for analysis and decision making. Overall, the integration of IoT technologies in EVCS improves the user experience and increases the efficiency of the charging infrastructure

Sensing, networking, and communication are the three pillars upon which the EVCS rests. The parts dealing with the interaction with people and making connections are the easiest to break into. The networking layer is responsible for coordinating communication with the Supervisory Control and Data Acquisition (SCADA). The communication layer is responsible for facilitating effective Internet-based communication between the EVCS and the user. This may be performed using a variety of technologies, including Bluetooth, Wi-Fi, cellular, and even regular Digital Subscriber Lines (DSL) or fiber optics. "Internal systems" relate to the rest of the EVCS, which includes things such as sensors and processors. The sensing layer is just as susceptible to attacks but under certain conditions. The sensing layer attacks need direct physical contact with the EVCS or may be abused in future stages once the EVCS's communication and networking component has already been breached. The

intruders may use the compromised EVCS as part of a covert botnet to launch coordinated attacks on other networks. Cyber insurance cost against attacks on EVCS was calculated in recent research, and it was found that cyberattacks on EVCS systems result in significant financial losses.

There are different potential types of attacks on Electric Vehicle Charging Stations (EVCS) that could compromise the security and integrity of the charging process, as well as the safety and privacy of users.

One type of attack is a physical attack, where an attacker could tamper with or damage the charging station hardware, potentially causing a fire or other safety hazard.

Another type of attack is a network-based attack, where an attacker could gain unauthorized access to the EVCS network and manipulate or disrupt the charging process. This could include attacks such as denial of service (DoS) attacks, where the attacker floods the network with traffic to prevent legitimate users from accessing the charging station, or man-in-the-middle (MitM) attacks, where the attacker intercepts and alters the communication between the charging station and the electric vehicle.

Additionally, attackers could target the payment systems used in EVCS to steal user information and financial data or manipulate the billing system to charge users for more than they consumed. Other types of attacks are related to the communication protocol used between EV and EVCS or vehicle-to-grid communication, where an attacker could intercept or manipulate the communication between the EV and EVSE or even the V2G communication. Finally, EVCS can be an entry point for attackers to target the overall electric grid infrastructure.

To mitigate these risks, EVCS manufacturers and operators can implement security measures such as encryption, firewalls, and intrusion detection systems, as well as regularly update the firmware and software of the charging stations. Additionally, following the guidelines and standards such as ISO/SAE 21434 and ISO 15118 can help to improve the overall cybersecurity of EVCS. The authors in [8] discussed the security requirements in EVCSs and their associated challenges. The main challenges revolve around the extended CIA triad, which includes Confidentiality, Integrity, Availability, Nonrepudiation, authenticity (message freshness), and Authentication. Figure 2 depicts the security requirements and their challenges in EVCSs. In addition, the corresponding attacks mapped to the main security requirements are illustrated in Figure 3.

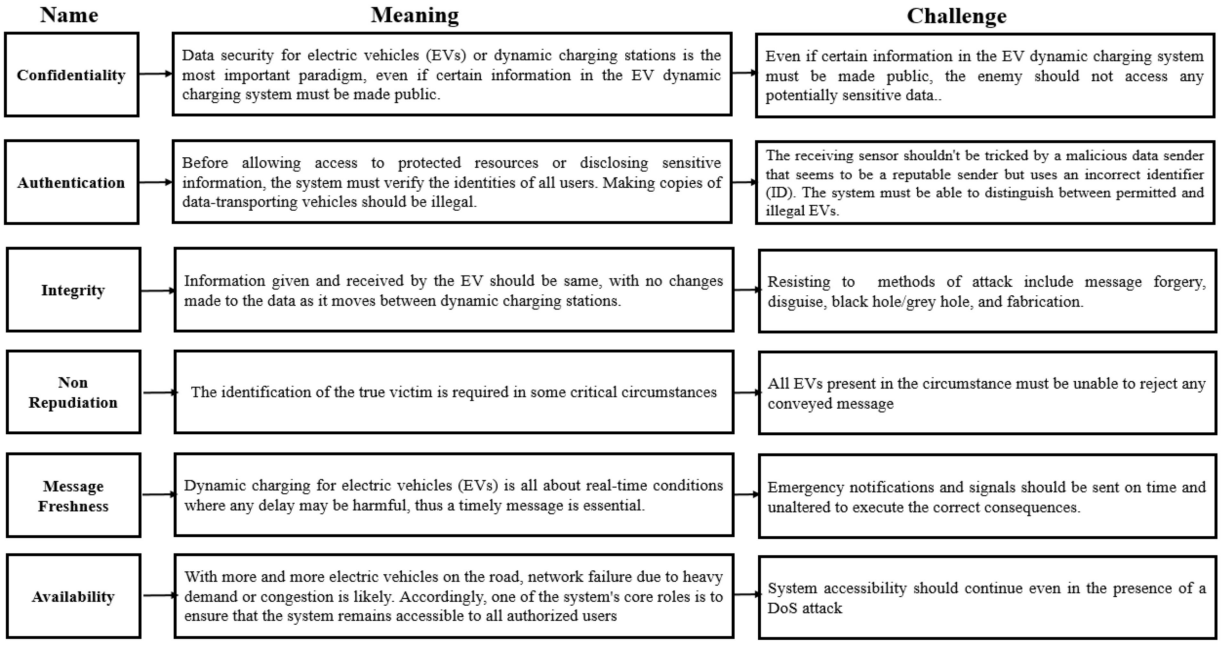

Figure 2. Security Requirements and their challenges in EVCSs.

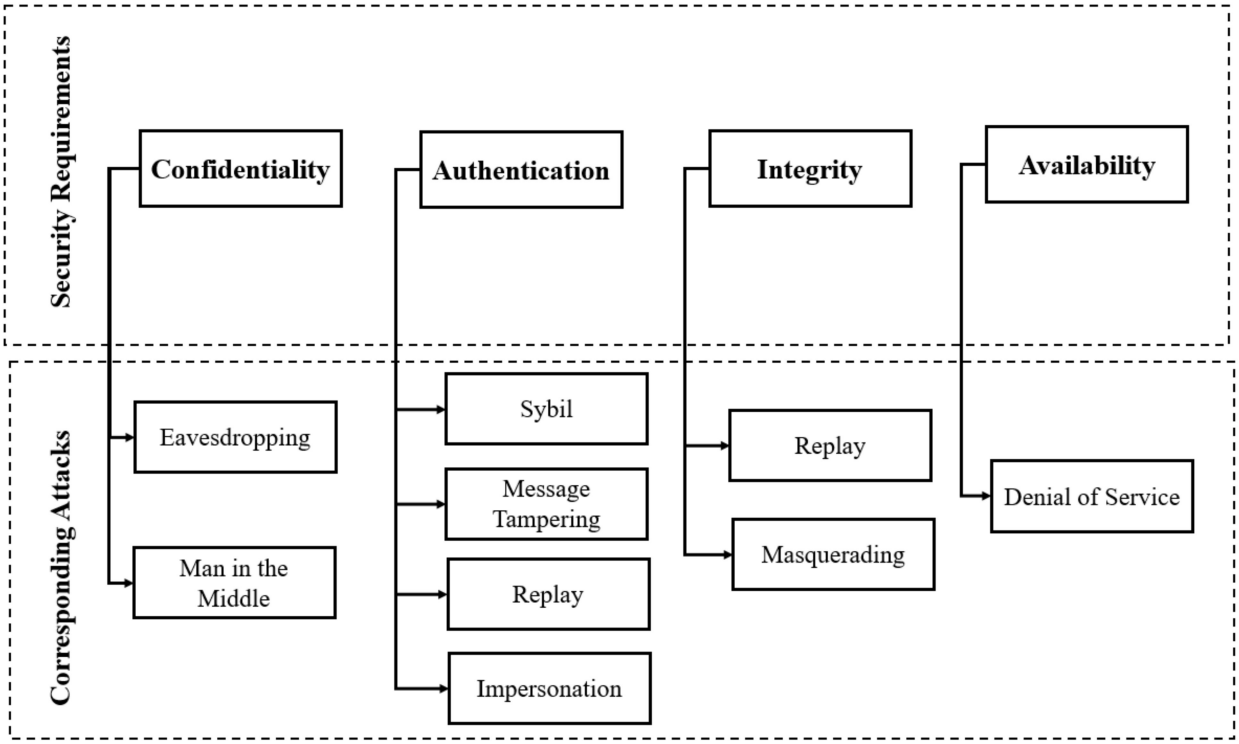

Figure 3. Security requirements and their corresponding attacks in EVCS.

3. Related Work

The integration of Artificial Intelligence (AI) into IDSs for IoT systems has been the focus of academic and commercial research efforts in recent years. Evidence suggests the combination of the two is most effective in identifying potentially malicious patterns of behavior. Machine learning methods such as Naive Bayes (NB), Logistic Regression (LR), and Decision Tree (DT) have all seen widespread usage in the detection of network-based threats. The methods are all based on the concept of learning from a labeled dataset. This is a common feature of data flowing between IoT devices. Deep Learning approaches have been the subject of further studies to increase accuracy and mitigate the effects of feature selection. The model's approach and data collection are essential in determining the relevance of its findings to the real world. Major online, mobile, and firmware zero-day vulnerabilities were discovered in an analysis of sixteen popular EVCSMS used by well-known companies, particularly in Europe and the United States [9]. They used the discovered vulnerabilities to gain unauthorized access to the EVCS, which caused power outages for the system's end customers. When compared to the security of other components of the EV ecosystem, the firmware and EVCSMS of EVCSs have received less attention from academics. The research in [10] quantified the severity of potential vulnerabilities in an operational EVCS. According to their results, there is a serious vulnerability in the live systems now used to charge EVs, which might have serious repercussions for the power grid and its consumers. Their study concluded with a set of preventative actions that may be implemented in vulnerable systems to decrease the impact of such attacks.

The authors in [11] proposed building an intrusion detection system using Deep Belief Networks (DBNs). It is a technique for enhancing the input to successive layers of architecture made up of different unsupervised networks. To do this, they employed auto encoders, specifically confined Boltzmann Machines (RBMs). After completing the training, they labeled events as either 0 (no intrusion detected) or 1 (intrusion detected). The 30,000-tuple TON IOT dataset was used in this model. This IoT dataset was developed in a controlled setting by the UNSW Canberra Cyber Range and IoT labs to mimic a medium-sized network in Australia. This dataset is known as the go-to source for a comprehensive collection of non-standard Internet of Things (IoT) risks. TensorFlow was used to create the

model's code. The data show that this model is 84% effective and has an F1 score of 84%. A notable aspect of the study is the comparison of DBN results to those acquired by other algorithms, which reveals that the DBN has lower accuracy (86%) than the Deep Neural Network (DNN) (96%) and the LSTM + CNN (97%), although performs better than the NB (54%) and the Support Vector Machine (SVM) (97%). Thakkar et al. [12] completed a comprehensive study on the usage of machine learning and deep learning techniques in IoT intrusion detection systems. Security issues and risks to the Internet of Things systems were outlined. Since denial-of-service (DoS) attacks inside the EVCS are a real possibility owing to the IoT system's open communication layer, the authors of [13] developed a deep-learning-based Intrusion Detection System (IDS) to detect them. They combined the DNN and Long Short-Term Memory (LSTM) neural network learning techniques. There was a 99% success rate with both approaches; however, the study concluded that the LSTM was superior. However, the research was narrowly focused on the Distributed Denial of Service (DDoS) attack. Using deep learning in a real-time setting, as suggested in [13], would be a waste of resources and, at most, would only uncover malicious behaviors after the traffic had already been routed across the network. Finally, the CICIDS 2018 dataset is not relevant to the IoT problems since it is not derived from pure IoT traffic.

The authors of [14] made use of the IoT-23 dataset by choosing a broad variety of Machine Learning methods. They compared the performance of the Random Forest (RF) algorithm to the Naive Bayes (NB) algorithm, the Multi-layer Perception (MLP) algorithm, the Support Vector Machine (SVM), and AdaBoost (ADA). The Random Forest approach has the highest accuracy (99.5%) compared to the other methods. Our results were consistent with those of the mentioned study as well as those of Thamataiselvi et al. [15].

Different IoT security issues examined in [16] included authentication, access control, safe offloading, and virus detection. They also researched different machine learning approaches in detail, including supervised, unsupervised, and Reinforcement Learning (RL), with the goal of using such algorithms on the constrained hardware of IoT devices.

As part of [17], a survey was conducted to assess the current use of IoT-ML in the medical field. According to research, the sensing layer is the weakest link on the Internet of Things. However, the authors did not discuss the dataset used by the ML algorithms. Different supervised and unsupervised ML approaches were compared using the CICIDS 2017 dataset in a benchmark study on anomaly detection in ML-based IDS [18]. ANN, DT, k-NN, NB, RF, SVM, CNN, EM, K-means, and SOM were examined in their benchmark study. The models had trouble spotting multi-classification attacks. A recent review on IDS based on ML and DL algorithms [19] used different datasets and found that the combination of the ML and DL with the different datasets produced promising results to achieve the highest accuracy, but the F1 and recall were not on the focus of the study, indicating that it is not a fair evaluation. According to the findings of the extensive study of IoT IDS reported in [20], in [21], the authors used Hierarchical Clustering Based on Dendrogram, which is a method used in sustainable transportation systems to group similar objects or elements into clusters. This method uses a dendrogram, a tree-like diagram, to represent the hierarchical structure of the clusters. In this approach, the objects are first considered as individual clusters, and then they are merged into bigger clusters based on their similarity. The dendrogram helps to visualize the relationships between the clusters and to determine the optimal number of clusters for the data. This method can be useful for identifying patterns and trends in transportation data, such as traffic flow or public transportation usage, and for making decisions about transportation infrastructure and planning.

It is hard to use DL's computing capacity in a constrained environment such as the IoT. However, offloading this capability to the edge or cloud may help mitigate part of the problem. Table 1 summarizes the comparison between the different approaches and datasets used in the literature surveyed in this paper. Based on this survey, Figure 4 compares the different datasets used for the same purpose.

Table 1. Comparison between the different approaches and datasets used to secure IoT systems.

Ref.	Method Used		Dataset			
	Machine Learning	Deep Learning	TON_IOT	CICIDS	IOT-23	KDD CUP 99
[11]	×	✓	✓	×	×	×
[12]	✓	✓	×	×	×	×
[13]	×	✓	×	✓	×	×
[14]	✓	×	×	×	✓	×
[15]	✓	×	×	×	✓	×
[16]	✓	×	×	×	×	✓
[17]	✓	×	×	×	×	×
[18]	✓	×	×	✓	×	×
[19]	✓	✓	✓	✓	✓	✓
[20]	✓	✓	✓	✓	✓	✓

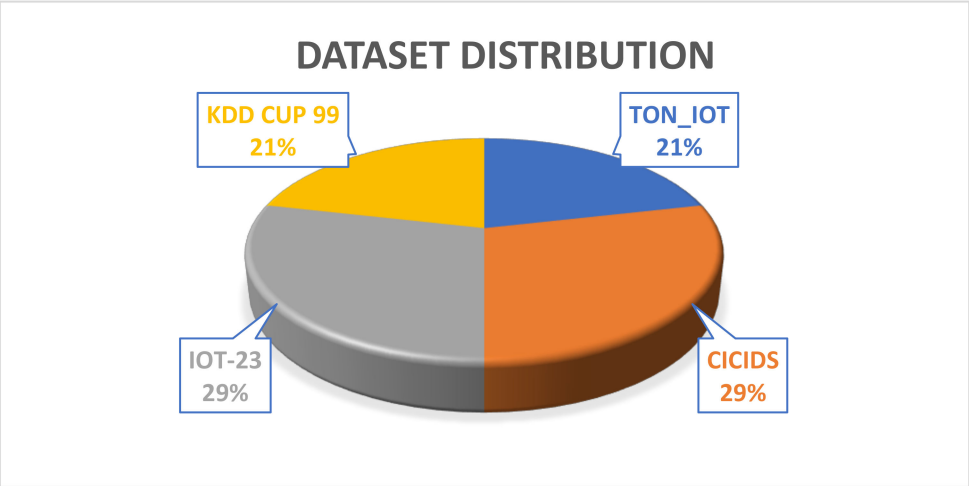

Figure 4. Dataset distribution used in the literature for securing IOT systems.

4. Experimental Approach

To verify an IDS, testing data are required. Due to security and privacy issues, it is difficult to gain genuine interest in commercial products. Datasets such as KDD, DRPA, NDS-KDD, and ADFA-LD are accessible. Scientists often use them as guides. For this, we use the IoT-23 Dataset. The most recent dataset, IoT-23 [15], was constructed from real-world commercial IoT network data. The IoT component here represents the EVCS as an IoT system. Twenty malicious and three benign traffic samples from IoT devices are included in the collection. The Stratosphere Lab of the Czech Republic, with help from Avast Software of Prague, published the dataset in 2020. The twenty scenarios that make up the IoT-23 dataset are meant to represent the malicious traffic that might result from different attacks on the IoT network. There are labels for every possible outcome. The IoT-23 dataset also features three examples of regular (i.e., not infected) Internet of Things traffic. IoT-23 refers to the overall number of cases, which is twenty-three.

On the other side, Machine Learning and Deep Learning have been widely employed recently to help find anomalies [22,23]. The difficulty lies in deciding which algorithm is the most suitable. The goal is a precise solution with little computational overhead. This helps with real-time attack detection and stopping dangerous communications. Machine learning classifiers must be accurate even when trained with a small number of data

points, meaning that they can make the right judgment with minimal data. Unsupervised learning algorithms are widely used to counteract unknown attacks (zero-day attacks). However, one of the drawbacks of using unsupervised learning algorithms is that they have a high false alarm rate and a low detection rate. To the best of our knowledge, the highest performance obtained by unsupervised learning techniques does not exceed 90%, which is insufficient for defending against unknown attacks. Implementing supervised learning algorithms, on the other hand, can achieve a high performance of 99% or higher. The obtained performance is comparable to signature-based intrusion detection systems (e.g., snort). To overcome this problem, regularization techniques are the solution to this dilemma. They can be used to simplify the system and overcome the overfitting problem in supervised learning [24], and thus supervised learning algorithms can outperform unsupervised learning algorithms for the same problem. Different regularization techniques, namely L1 and L2 [25], have been used to address the issue of overfitting and improve the detection capability of network-based intrusion detection systems. When developing more comprehensive models, it is also important to avoid overfitting the data, which is why randomization of the data is required. To maintain uniformity, we subjected the same reshuffled dataset to two classification algorithms described hereafter. Decision Table classifiers and the Filtered Classifier were examined, and the results were captured.

Decision Table classifier rules are described as building and using a simple decision table majority classifier. The output shows a decision on different attributes for each instance. The number and specific types of attributes can vary to suit the needs of the task.

The Filtered Classifier, on the other hand, filters out the irrelevant data in favor of the important stuff [26]. The time required for computations and the effectiveness of algorithms will be affected. Attribute selection is performed before more advanced methods such as classification, clustering, etc. Attributes are chosen in sequential order in two parts. As the first step, subset generation makes use of searching to evaluate both the determined and potential subsets. The top performers have more value. This process must be repeated until completion. Step two is ranking, which involves utilizing either statistics or information theory to establish the relative weight of qualities [27].

Machine learning algorithms typically learn from a dataset, where separate sets of data are used for training and testing. Dataset characteristics are learned and analyzed in the training set, while algorithms are taught to use characteristics from a given dataset to determine if a given sample is malicious or not. ML improves classification accuracy by analyzing normal and malicious traffic. Classification and clustering are ML methods, where classification algorithms use labelled data samples to predict the output by studying input parameters. These strategies construct input–output relationships. The training set is used to train the classification algorithm's learning model. New data are predicted and classified based on what was learned during the training phase.

In our simulation, the data are divided into two samples, namely, a training sample and a testing sample. The training sample undergoes the pattern analysis and then label learning by the machine learning process, while in the testing phase, the labels are hidden from the model, and the classification engine classifies the unlabeled data based on the machine learning process that was performed in the training phase. The outcome of the classification process in the testing phase is the labels predicted by the learned model, as illustrated in Figure 5, which shows the experimental approach and methodology used in building the simulation. The Proposed IDS will be placed at the EVCSMS (as the central point) to monitor all the traffic between the distributed EVCSs and the EVCSMS.

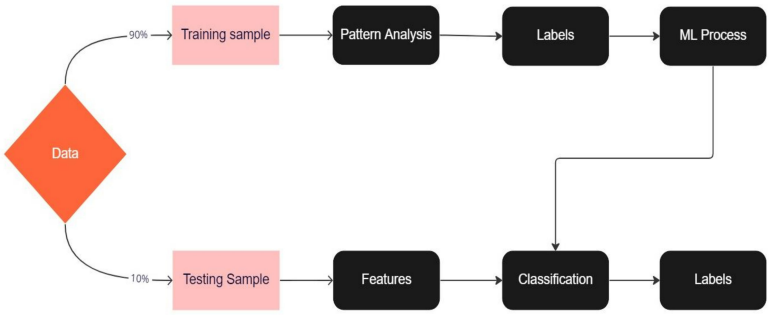

Figure 5. Simulation's Experimental Approach and Methodology.

5. Simulation Results

Our proposed binary classification model examines the accuracy of the system with 124,000 flows distributed between benign and DDOS attack flows. The distribution of the DDOS attack flows versus the benign traffic is 51,361 (DDOS)/73,085 (benign). We obtain a total of approximately 124 K flows, in which 90% of the flows (111 K) were used in training the system, where 10%, i.e., 12 K flows, was used in evaluating the system. The algorithm's speed and accuracy were measured, as well as its precision, recall, and F-1 score.

Figure 6 depicts the modelling time for the Decision Table, which takes 61.6 s, while it takes only 0.75 s to model the Filtered Classifier. Figure 7 illustrates the higher performance of the Filtered Classifier over the Decision Table in terms of accuracy (99.99% versus 99.97%). The binary classification algorithm with the highest accuracy was the Filtered Classifier (99.99%). The Filtered Classifier modeling time (0.75 s) was much quicker than the Decision Table classifier (61.6 s). This is because the Filtered Classifier runs in parallel, while the Decision Table classifier is sequential. The Filtered Classifier method assesses each class independently and in parallel (two distinct chunks of parallel operations). Figure 7 shows a comparison of the precision, recall, and F-1 Score of the Decision Table classifier versus the Filtered Classifier. When compared to cutting-edge methods such as those reported in [19,20], the Filtered Classifier exceeds the other Deep learning algorithms (maximum accuracy of 97%). Its accuracy is 99.99 percent.

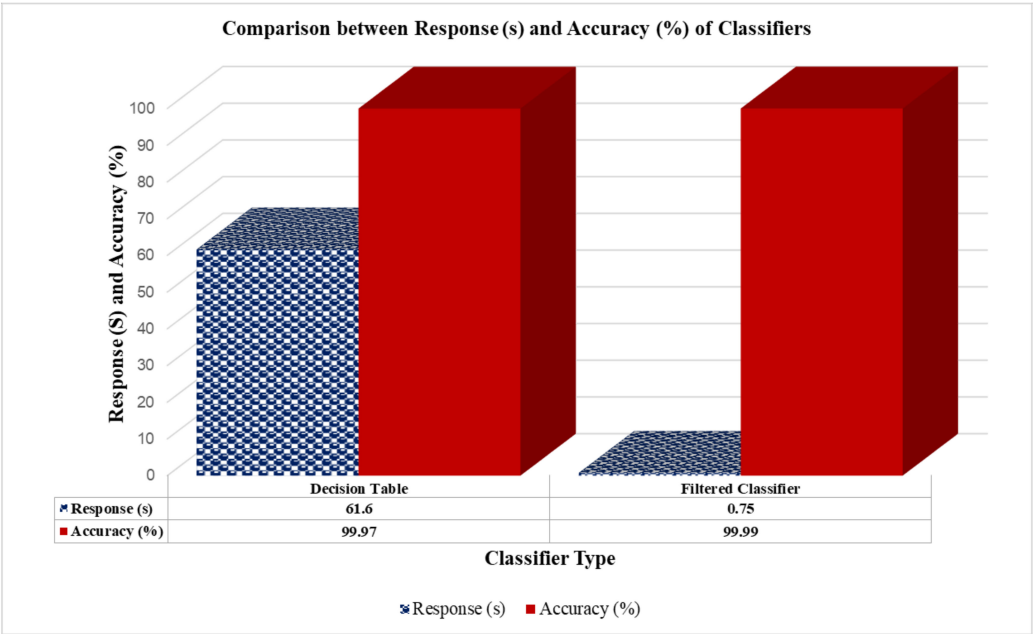

Figure 6. Accuracy and response comparison for the Decision Table and Filtered Classifier algorithms.

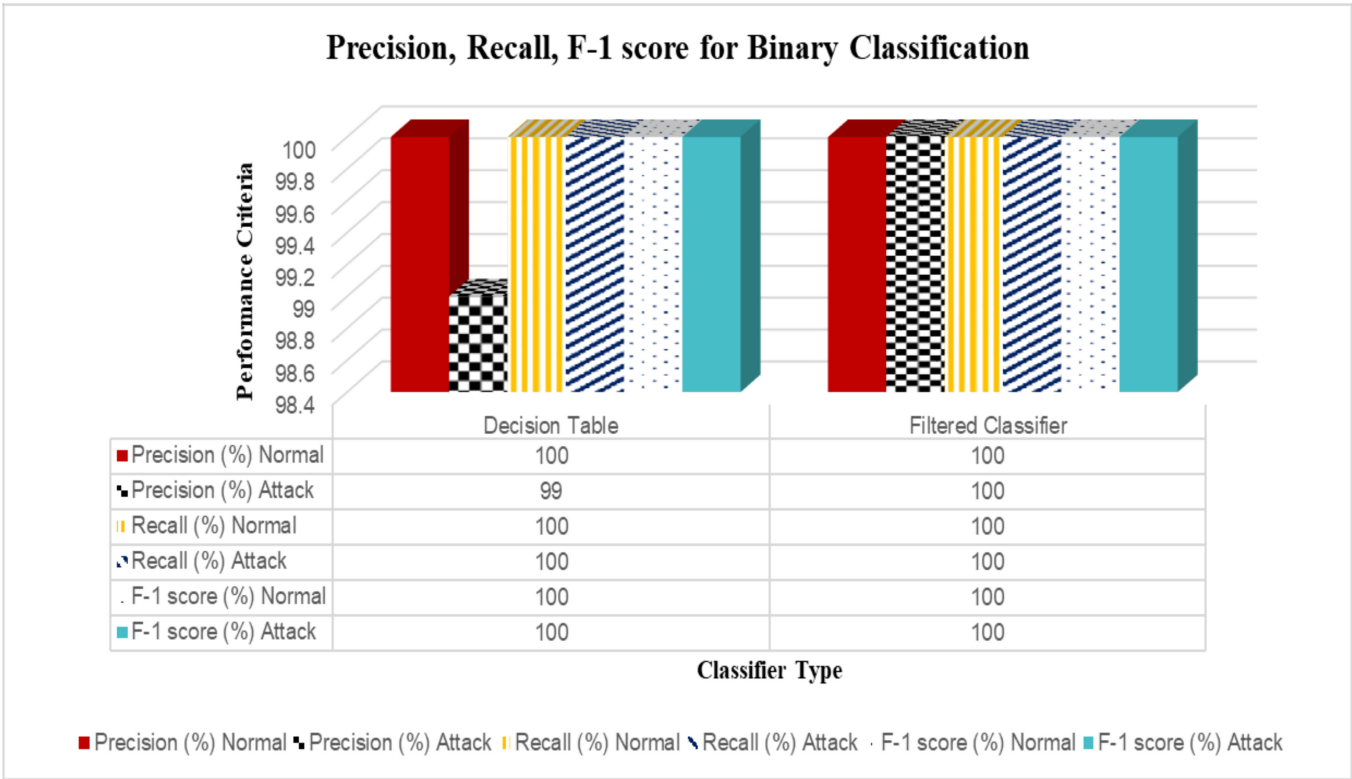

Figure 7. Precision, Recall, and F-1 Score for the Decision Table versus the Filtered Classifier.

The filtered classifier algorithm is better than the decision table classifier algorithm in certain situations because it can manage large amounts of data and is able to handle missing attribute values. Additionally, the filtered classifier algorithm can also handle noisy data, which can often lead to more accurate classification results. The decision table classifier algorithm, on the other hand, may not perform as well on large datasets or when there are missing attribute values or noisy data. The filtered classifier algorithm is generally faster than the decision table classifier algorithm for different reasons. One reason is that the filtered classifier algorithm uses a subset of the features (attributes) to make predictions, whereas the decision table classifier algorithm uses all the features. Using a subset of features can reduce the amount of computation required to make predictions, which can make the filtered classifier algorithm faster. Additionally, the filtered classifier algorithm can leverage machine learning techniques such as feature selection and ensemble methods to improve the performance of the classifier, which can lead to faster predictions. On the other hand, the decision table classifier algorithm uses all the features and can be slow when dealing with large and complex datasets.

6. Discussion and Limitations

The issue of EVCS security is a genuine industrial concern. If exploited by malicious actors and state-sponsored attack groups, a cyberattack on the EVCS may have disastrous effects. Due to the limited number of EVCSs already deployed and the growing number of Electric Vehicles with a short battery range, any outage in a single EVCS has the potential to disrupt the travel plans of EV users. In addition, an entire power grid can be shut down by a cyberattack, which can have a direct impact on the economy. To limit this danger, a precise and effective intrusion detection system is required. In this study, the use of machine learning to construct the IDS engine is explored. To accurately evaluate the suggested IDS, a dataset that accurately reflects the actual traffic and assaults may be required. This study evaluates two machine learning (ML)-based intrusion detection system (IDS) classifier methods using the IoT-23 dataset, which is comprised of native IoT network traffic. Each

classifier's theory of operation is based on a distinct set of premises. We observed from the findings that the filtered classifiers perform exceptionally well in terms of accuracy and other metrics on the testing data. Therefore, it can be utilized to protect the EVCS network against DDoS attacks.

However, the following limitations are present in our research:

1. Although Deep Learning (DL) is widely employed in a variety of application domains, such as image pre-processing and language translation, it is beyond the scope of this work.
2. Without installing a physical EVCS system, we trained and assessed the ML algorithms offline via virtual simulation. However, it is crucial to understand how this IDS handles intrusions in real-time by detecting internet threats.
3. When conducting an intrinsic evaluation, we should compare different datasets. In this study, however, we solely used the IoT-23 dataset to train and assess various ML algorithms. We intend to compile our own dataset from an actual EVCS system and evaluate multiple datasets to develop a viable intrusion detection algorithm.

7. Conclusions and Future Work

In this paper, we discussed the EVCS security requirements, threats, and challenges. We compared different approaches used in the literature to address the different types of threats affecting the EVCS/IoT systems. We also presented the usage of the various datasets in recent research papers. We applied machine learning methods to be used in anomaly-based IDSs with high accuracy. We evaluated two traditional classifiers used in Machine learning: The Decision Tree Classifier and the Filtered Classifier. The Filtered Classifier has the best performance in binary classification in terms of accuracy, precision, recall, F-1 score, and modeling time, making it the best solution for identifying DDoS attacks in the IoT Environment. These results are in line with those of previous studies. The suggested method may be used to enhance the security of any sensitive Industrial Control Systems (ICSs), ranging from SCADA to green hydrogen control systems. By highlighting the need for training classification models on appropriate datasets, we hope that the results of this research will contribute to the development of a complete IDS. In this paper, we minimized the training data used in the simulations and observed the accuracy of the intrusion detection system. The results proved that the detection accuracy was not affected. This should help in identifying malicious traffic with minimal training data, which increases the agility of the EVCS IDS. In the future, we plan to investigate the role of feature selection and other deep learning techniques. We will focus on the Deep Learning algorithms, and various datasets will be used to assess IDS efficiency.

Author Contributions: Methodology, M.E.; Validation, M.A.A.; Formal analysis, M.E.; Resources, M.S.E.; Writing—original draft, M.E.; Visualization, M.A.A.; Supervision, H.A., M.S.E. and A.D.J.; Funding acquisition, A.D.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Dataset used can be downloaded from https://www.stratosphereips.org/datasets-iot23.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Suriya, N.; Shankar, S.V. A novel ensembling of deep learning based intrusion detection system and scroll chaotic countermeasures for electric vehicle charging System. *J. Intell. Fuzzy Syst.* **2022**, *43*, 4789–4801. [CrossRef]
2. Kumar, T.; Kumar, N.; Thakur, T.; Nema, S. Charge scheduling framework with multiaggregator collaboration for direct charging and battery swapping station in a coupled distribution-transportation network. *Int. J. Energy Res.* **2022**, *46*, 11139–11162. [CrossRef]
3. Yoshioka, K. Fighting iot cyberattacks: Device discovery, attack observation and security notification. In Proceedings of the 8th ACM on CyberPhysical System Security Workshop, Nagasaki, Japan, 30 May 2022; pp. 39–40.

4. El Houda, Z.A.; Brik, B.; Khoukhi, L. "Why should I trust your ids?": An explainable deep learning framework for intrusion detection systems in internet of things networks. *IEEE Open J. Commun. Soc.* **2022**, *3*, 1164–1176. [CrossRef]
5. Sarhan, M.; Layeghy, S.; Portmann, M. Towards a standard feature set for network intrusion detection system datasets. *Mob. Netw. Appl.* **2022**, *27*, 357–370. [CrossRef]
6. Otoum, Y.; Liu, D.; Nayak, A. Dl-ids: A deep learning–based intrusion detection framework for securing iot. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e3803. [CrossRef]
7. Blakely, B.; Kurtenbach, J.; Nowak, L. Exploring the information content of cyber breach reports and the relationship to internal controls. *Int. J. Account. Inf. Syst.* **2022**, *46*, 100568. [CrossRef]
8. Babu, P.R.; Basker, P.; Alavalapati, G.R.; Vanga, O.; Hyun, S.K. A survey on security challenges and protocols of electric vehicle dynamic charging system. *Secur. Priv.* **2022**, *5*, e210. [CrossRef]
9. Su, Q.; Wang, H.; Sun, C.; Li, B.; Li, J. Cyber-attacks against cyberphysical power systems security: State estimation, attacks reconstruction and defense strategy. *Appl. Math. Comput.* **2022**, *413*, 126639.
10. Nasr, T.; Torabi, S.; Bou-Harb, E.; Fachkha, C.; Assi, C. Power jacking your station: In-depth security analysis of electric vehicle charging station management systems. *Comput. Secur.* **2022**, *112*, 102511. [CrossRef]
11. Malik, R.; Singh, Y.; Sheikh, Z.; Anand, P.; Singh, P.; Workneh, T.C. An improved deep belief network ids on iot-based network for traffic systems. *J. Adv. Transp.* **2022**, *2022*, 7892130. [CrossRef]
12. Thakkar, A.; Lohiya, R. A review on machine learning and deep learning perspectives of ids for iot: Recent updates, security issues, and challenges. *Arch. Comput. Methods Eng.* **2021**, *28*, 3211–3243. [CrossRef]
13. Basnet, M.; Ali, M.H. Deep learning-based intrusion detection system for electric vehicle charging station. In Proceedings of the 2020 2nd International Conference on Smart Power & Internet Energy Systems (SPIES), Bangkok, Thailand, 15–18 September 2020; pp. 408–413.
14. Stoian, N.-A. Machine Learning for Anomaly Detection in Iot Networks: Malware Analysis on the Iot-23 Data Set. Bachelor's Thesis, University of Twente, Enschede, The Netherlands, 2020.
15. Thamaraiselvi, D.; Mary, S. Attack and anomaly detection in iot networks using machine learning. *Int. J. Comput. Sci. Mob. Comput.* **2020**, *9*, 95–103. [CrossRef]
16. Xiao, L.; Wan, X.; Lu, X.; Zhang, Y.; Wu, D. Iot security techniques based on machine learning: How do iot devices use ai to enhance security? *IEEE Signal Process. Mag.* **2018**, *35*, 41–49. [CrossRef]
17. Sworna, N.S.; Islam, A.; Shatabda, S.; Islam, S. Towards development of iot-ml driven healthcare systems: A survey. *J. Netw. Comput. Appl.* **2021**, *196*, 103244. [CrossRef]
18. Maseer, Z.K.; Yusof, R.; Bahaman, N.; Mostafa, S.; Foozy, C.F.M. Benchmarking of machine learning for anomaly based intrusion detection systems in the cicids2017 dataset. *IEEE Access* **2021**, *9*, 22351–22370. [CrossRef]
19. Amanoul, S.V.; Abdulazeez, A.M. Intrusion detection system based on machine learning algorithms: A review. In Proceedings of the 2022 IEEE 18th International Colloquium on Signal Processing & Applications (CSPA), Selangor, Malaysia, 12 May 2022; pp. 79–84.
20. Ahmad, R.; Alsmadi, I.; Alhamdani, W.; Tawalbeh, L. A comprehensive deep learning benchmark for iot ids. *Comput. Secur.* **2022**, *114*, 102588. [CrossRef]
21. Sangaiah, A.K.; Javadpour, A.; Ja'fari, F.; Zhang, W.; Khaniabadi, S.M. Hierarchical Clustering Based on Dendrogram in Sustainable Transportation Systems. *IEEE Trans. Intell. Transp. Syst.* **2022**. [CrossRef]
22. Balaji, R.; Deepajothi, S.; Prabaharan, G.; Daniya, T.; Karthikeyan, P.; Velliangiri, S. Survey on intrusions detection system using deep learning in iot environment. In Proceedings of the 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 7–9 April 2022; pp. 195–199.
23. Zeadally, S.; Tsikerdekis, M. Securing internet of things (iot) with machine learning. *Int. J. Commun. Syst.* **2020**, *33*, e4169. [CrossRef]
24. Ying, X. An overview of overfitting and its solutions. In *Journal of Physics: Conference Series*; IOP Publishing: Bristol, UK, 2019; Volume 1168, p. 022022.
25. Aljawarneh, S.; Yassein, M.; Aljundi, M. An enhanced j48 classification algorithm for the anomaly intrusion detection systems. *Clust. Comput.* **2019**, *22*, 10549–10565. [CrossRef]
26. Gnanambal, S.; Thangaraj, M.; Meenatchi, V.; Gayathri, V. Classification algorithms with attribute selection: An evaluation study using weka. *Int. J. Adv. Netw. Appl.* **2018**, *9*, 3640–3644.
27. Handa, A.; Semwal, P. Evaluating performance of scalable fair clustering machine learning techniques in detecting cyber-attacks in industrial control systems. In *Handbook of Big Data Analytics and Forensics*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 105–116.