Securing EVCS Infrastructure Against Cyberattacks with a Deep Learning-Based Detection Model

Md Rakibul Ahasan
Electrical and Computer Engineering
Florida State University
Tallahassee, FL, USA
mahasan@fsu.edu

Shahriar Rahman Fahim
Electrical and Computer Engineering
Texas A&M University
College Station, TX, USA
sr-fahim@tamu.edu

Abdulrahman Takiddin
Electrical and Computer Engineering
Florida State University
Tallahassee, FL, USA
a.takiddin@fsu.edu

***Abstract*—The rapid growth of electric vehicles (EVs) necessitates the development of secure and efficient electric vehicle charging stations (EVCSs), which, when integrated with smart grid (SG) technology, become critical components of smart city infrastructure. However, EVCSs remain vulnerable to cyberattacks, such as charging profile alteration attacks (CPAAs), where malicious actors manipulate parameters like start time, end time, and energy demand, causing disruptions in charging processes and SG instability. This study introduces a robust detection model based on a convolutional attention autoencoder network (CAENet) model, which integrates a deep autoencoder for dimensionality reduction, convolutional layers for feature extraction, and an attention mechanism to prioritize critical temporal features. The model is trained on a realistic EVCS charging data to identify CPAAs by effectively capturing temporal dependencies. The CAENet model offers 94% detection rate against CPAAs, outperforming benchmark machine learning approaches by $7-12\%$.**

***Index Terms*—Cyber-physical systems, deep autoencoder, electric vehicles, electric vehicle charging stations, and intelligent transportation systems.**

I. Introduction

The adoption of electric vehicles (EVs) is growing globally, driving an increased demand for reliable and secure electric vehicle charging stations (EVCSs). EVCSs, often powered by Internet of Things (IoT) technologies, present a new frontier for cyberattacks. As critical components of smart city infrastructure and intelligent transportation systems, EVCSs integrate the smart grid (SG), EVs, and end-users through bidirectional data exchanges, making them cyber-physical systems (CPSs) [1]. However, the increasing reliance on such integrated systems exposes EVCSs to vulnerabilities that could be exploited by cyberattackers to disrupt charging operations or compromise user personal and financial data. In several documented incidents, attackers have exploited vulnerabilities in EVCS, leading to significant operational and financial losses. For example, a recent cyberattack on an EV charging infrastructure in Europe caused multiple stations to shut down, denying service to users for several hours [2]. Cyberattackers could also manipulate charging prices to encourage such behaviors, exacerbating the problem in a stealthy manner that is challenging to detect. Such instances emphasize the urgent need for robust security measures to safeguard EVCSs against evolving cyber threats. The rise in EV adoption has also necessitated the development of robust charging coordination mechanisms to prevent SG strain and reduce driver wait times. However, such mechanisms are vulnerable to distributed denial of charge (DDoC) attacks, where adversaries exploit legitimate access to overwhelm the system with fake charging requests. Such attacks disrupt service availability, increase costs, and compromise user convenience [3]. EVs and EVCSs communicate using Vehicle-to-Grid (V2G) protocols to manage charging sessions, which introduces vulnerabilities where malware can spread between vehicles and charging stations. The spread of malware has the potential to escalate into botnets, causing widespread disruptions such as power outages and traffic congestion. Additionally, integrating EVCSs into SG infrastructure has introduced vulnerabilities to various cyberattacks, such as false data injection attacks (FDIAs) and charging profile alteration attacks (CPAAs).

A. Related Works

To detect the aforementioned threats, machine learning (ML) and deep learning (DL)-based approaches leveraging historical and real-time data have been studied for attack detection in both, EVCS [4] and SG [5] domains as follows.

1) Attack Detection in EVCS: A support vector machine (SVM) model was employed to classify point-to-point energy transaction data and provided a 91% precision score by maximizing the hyperplane margin, but such a model was constrained by its dependence on linearly separable datasets, limited scalability for larger systems, and insufficient resilience against sophisticated cyberattacks [6]. A random forest (RF)-based detection mechanism achieved a 98% accuracy score against price manipulation attacks, but the model did not consider the temporal dependencies and high-level nonlinear interactions inherent in EVCS network [7]. An autoencoder-based framework was designed to detect FDIAs in energy markets by analyzing manipulated EVCS charging profiles and achieved a 91% accuracy score, but it struggled with imbalanced datasets, limiting its real-world applicability [8]. A convolutional neural network (CNN) model was proposed to detect distributed denial of service (DDoS) and FDIA attacks via scalogram images and achieved a 99% accuracy

score, but the model encountered difficulties detecting novel attack patterns, highlighting robustness limitations [9]. A long short term memory (LSTM) model was developed for attack detection at EVCS and achieved 99% accuracy, but the model is depended on specialized, high-fidelity data may impact real world scalability [10]. A temporal convolutional network model was developed for detecting cyber attacks on the EVCS interface connecting towards EV and achieved a 93% accuracy score when identifying multiple attack types, but the model detection applicability is constrained to the testbed environment [11].

2) Attack Detection in SGs: A recurrent neural network (RNN) model was proposed for electricity theft detection in advanced metering infrastructure (AMI) and achieved a 94% detection rate (DR) [12]. Deep autoencoders (DAEs) were introduced for anomaly detection. For example, variational autoencoders (VAEs), leveraging LSTMs to capture temporal patterns in AMI networks, achieved a 91% DR [13]. An autoencoder-bidirectional gated recurrent unit model achieved a 90% accuracy score [14]. An attention-enhanced autoencoder combined with an LSTM achieved a DR of 94% [15]. A graph autoencoder achieved a 98% DR on a 2000-bus system by analyzing spatiotemporal power and traffic data [4].

The challenges associated with the integration of EVCSs and SG as well as the limitations of existing works motivate the need for developing a resilient attack detection system against cybersecurity threats in such complex CPSs. Specifically, existing studies lack at least one of the following aspects: (a) capturing the spatiotemporal dependencies in the data, (b) adopting real datasets for training and testing to mimic realistic and practical scenarios, and (c) examining the impact of complex attack strategies (e.g., CPAAs) against ML-based detectors. This work overcomes the aforementioned limitations by introducing a CAEnet, which offers the advantages described next.

B. Problem Definition and Contributions

Operating as interconnected CPS, EVCS networks integrate SGs, EVs, and IoT devices to facilitate energy distribution and data exchange. One threat is CPAAs, which exploit the temporal dependencies in charging patterns, disrupting system operations and compromising user data. To address CPAAs, we introduce a robust attack detection model leveraging temporal dependencies in EVCS data for enhanced resilience against cyberattacks. Our contributions include:

1) We introduce a detection model, namely, convolutional attention autoencoder network (CAENet), combining a DAE for anomaly detection, a CNN for spatial feature extraction, and an attention mechanism to capture critical temporal dependencies.
2) We design an attack simulation function, namely, CPAA to emulate real-world cyberattacks on EV charging sessions by altering start times, end times, and energy demands, targeting a fraction of stations for robust evaluation.
3) The introduced CAENet model achieves a DR of 94% against CPAAs, surpassing benchmark ML-based approaches by 7–12% due to its ability in efficiently capturing temporal and spatial dependencies.

The remainder of this paper is organized as follows. Section II describes the EVCS system architecture as a CPS, detailing its physical and cyber layers. Section III introduces the dataset, including preprocessing, attack simulation strategies, and techniques for generating realistic cyberattack scenarios. Section IV outlines the details of the architecture and components of the CAENet model. Section V presents and analyzes the experimental results, including a performance comparison with benchmark models. Finally, Section VI concludes the paper by summarizing the findings and discussing future directions for enhancing EVCS security.

II. System Description

EVCSs serve as a hub where the physical (energy) and cyber (data/control) components intersect, creating a CPS. The goal is to ensure efficient, reliable, and secure power distribution for charging while protecting the system from cyberattacks that target both the physical and cyber layers of the system [16]. The physical layer and cyber layer are illustrated in Fig. 1 and are explained next.

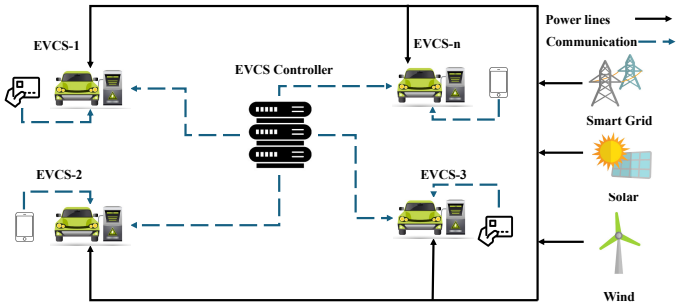

Fig. 1. CPS architecture of EVCS system.

A. Physical Layer

The physical layer of the EVCS system consists of three main elements. First, EVCSs, equipped with sensors to monitor the state of charge, voltage, and current, present the primary interface where vehicles plug in for charging. Second, renewable energy sources (RESs), including solar panels, wind energy, provide renewable energy to the EVCS, contributing to its sustainability. Third, power lines and transformers are responsible for facilitating energy transmission between the SG, RESs, and the EVCSs.

B. Cyber Layer

The cyber layer of the EVCS system comprises three main elements. First, control systems and sensors are responsible for managing energy flow, monitoring system status, and facilitating communication between components using protocols such

as the open charge point protocol. Second, communication networks enable secure data exchange between the EVCS, RESs, SG operators, and vehicles, leveraging supervisory control and data acquisition (SCADA) systems to ensure seamless integration. Third, intrusion detection and security systems utilize ML models to detect anomalies in network traffic and prevent cyberattacks. These security measures are often implemented in cloud-based EVCS control systems, enhancing the overall management and resilience of the EVCS infrastructure.

III. Data Preparation

To conduct our experiments, we adopt the adaptive charging network (ACN) dataset [17], which was collected from a campus garage in Pasadena, California, USA that provides information on EV connection times, charging durations, energy consumption, and day-specific details collected from a parking lot with 59 EVCSs. Such a dataset is adopted in this work as it includes critical features required to simulate CPAAs and evaluate detection mechanisms. Each EVCS corresponds to an EV charging point, with charging requests authenticated manually or via smartphones. Key features include charging start time, charging end time, charging duration, EVCS station ID, and the power consumed by the EV during the charging session.

A. Dataset Processing

The dataset includes $14,194$ charging session data over six months. The dataset exhibits benign samples only (i.e., readings during system normal operation) with a class label of "0". To generate attack samples, we employ the attack function described in the next subsection, which results in $2,677$ attack samples with a class label of "1", leading to a class imbalance, and potentially, bias attack detection results. To address the class imbalance issue, we employ the synthetic minority oversampling technique (SMOTE) [18] and the adaptive synthetic sampling approach (ADASYN) [19]. We employ SMOTE to generate synthetic samples for the minor class (i.e., attack samples) and balance the training data, while ADASYN adaptively creates more samples for harder-to-learn regions. This combined approach improves the accuracy and sensitivity of the models when classifying both classes. We then use 80% of the data for training and 20% for testing the models.

B. Attack Function and Strategies

In this work, we develop an attack function that simulates various types of cyberattacks on EV charging session data by modifying specific session attributes in the ACN dataset. The function applies a combination of start time increases, end time decreases, and energy demand changes to randomly selected charging sessions, assigning unique attack types based on the combination of these modifications. The parameters used in the attack are defined as follows: the start time increase ΔT_{start}, the end time decrease ΔT_{end}, and the energy demand change factor ΔE_{demand} are expressed as percentages of their respective values to allow dynamic adjustments. For each session i in a randomly selected set of attacked stations, the function applies one or more of the following attack types. The session's start time, t^i_{start}, is increased such that:

$$t^i_{\text{start\_new}} = t^i_{\text{start}} + (\Delta T_{\text{start}} \cdot t^i_{\text{start}}).$$

The session's end time, t^i_{end}, is decreased such that:

$$t^i_{\text{end\_new}} = t^i_{\text{end}} - (\Delta T_{\text{end}} \cdot t^i_{\text{end}}).$$

Finally, the energy delivered, $E^i_{\text{delivered}}$, is increased by ΔE_{demand}, resulting in:

$$E^i_{\text{delivered\_new}} = E^i_{\text{delivered}} \times (1 + \Delta E_{\text{demand}}).$$

The attack function assigns each session a single attack type or a combination of attack types, as described in Table I alongside its session count. The attacks range from individual modifications, such as types 1, 2, and 3, or combining modifications such as types 4 and 5. Such a combination of attacks is particularly stealthy as they introduce complex deviations that closely mimic natural variations in charging behavior, making them harder to detect. By incorporating these diverse attack types, the attack function ensures a comprehensive evaluation of the detection model's robustness.

TABLE I
Description of the Launched Attack Types

Type	Count	Attack detail
1	547	Start time is increased
2	538	End time is decreased
3	514	Energy demand is increased
4	527	Start time and energy demand are changed
5	551	Start time, end time, and energy demand are changed

The process described in Algorithm 1 modifies the daily session data from EVCSs with targeted alterations to simulate cyberattacks. Each day, d, a subset of charging stations, denoted as $S_{\text{attack}} \subseteq S_d$, is selected for attack based on the total number of stations available. The number of stations chosen for attack each day is calculated as $|S_{\text{attack}}| = \max(1, \lfloor r \times |S_d| \rfloor)$, where r is the fraction of stations attacked per day determined by the attacker's strategy, ensuring that at least one station is always attacked. For each selected station $s \in S_{\text{attack}}$, one or more attack types are applied to modify session attributes such as start time t_{start}, end time t_{end}, and delivered energy $E_{\text{delivered}}$. These modifications offer a realistic representation of potential cyberattack impacts on EVCS infrastructure, generating valuable data for analyzing security vulnerabilities and evaluating resilience strategies.

IV. Detection Models

Anomalies in EV charging session data pose significant challenges for ensuring reliability and efficiency in EV infrastructure. To address these challenges, we introduce the CAENet model, a hybrid deep learning framework that integrates a DAE, CNNs, and an attention mechanism. Our model is designed to effectively capture spatial and temporal patterns as well as prioritizing critical features through its attention mechanism, enabling robust attack detection. We also compare

Algorithm 1: Daily attack selection

Input: Dataset with daily charging session data
Output: Modified dataset with attack labels

for *each day* d *in dataset* **do**
  Identify the set of unique stations S_d;
  Determine $|S_{\text{attack}}| = \max(1, \lfloor r \times |S_d| \rfloor, \quad \text{where } S_{\text{attack}} \subseteq S_d$;
  for *each station* $s \in S_{attack}$ **do**
    Randomly select attack types: increase t_{start}, decrease t_{end}, increase demand;
    Apply selected attack types to sessions at s;

our CAENet model to benchmark detectors for performance comparisons.

A. CAENet Model

Our CAENet detection model introduces a hybrid deep learning model combining a DAE, CNNs, and an attention mechanism to detect attacks effectively in EV charging session data. The optimization process plays a vital role in ensuring robust performance by jointly minimizing reconstruction and classification losses while emphasizing significant temporal features through the attention mechanism. The model begins with a DAE for dimensionality reduction, compressing the input data $\mathbf{x} \in \mathbb{R}^n$, where n is the number of input features into a latent representation $\mathbf{z} \in \mathbb{R}^m$, where m is the size of the latent space:

$$\mathbf{z} = \sigma(\mathbf{W}_{\text{enc}}\mathbf{x} + \mathbf{b}_{\text{enc}}), \tag{1}$$

where, σ is the activation function, $\mathbf{W}_{\text{enc}}$ is the weight and $\mathbf{b}_{\text{enc}}$ is the bias of the encoder layer of DAE. The latent representation $\mathbf{z}$ then passes through the decoder layer of DAE, and a reconstruction of input data $\hat{\mathbf{x}}$ is prepared as:

$$\hat{\mathbf{x}} = \sigma(\mathbf{W}_{\text{dec}}\mathbf{z} + \mathbf{b}_{\text{dec}}), \tag{2}$$

where, $\mathbf{W}_{\text{dec}}$ is the weight and $\mathbf{b}_{\text{dec}}$ is the bias of the decoder layer of DAE. The reconstruction loss $\mathcal{L}_{\text{recon}}$ quantifies the discrepancy between the input $\mathbf{x}$ and its reconstruction $\hat{\mathbf{x}}$, ensuring that the latent representation effectively preserves the input's essential features is defined as:

$$\mathcal{L}_{\text{recon}} = \frac{1}{n}\sum_{j=1}^{n} \|\mathbf{x}_j - \hat{\mathbf{x}}_j\|_2^2, \tag{3}$$

where j is the index over the input feature, i.e., $j = 1, 2, \ldots, n$. The latent representation $\mathbf{z}$ is passed through convolutional layers to extract spatial and temporal features. A single convolution operation is defined as:

$$y[p] = \sum_{q=1}^{k} \mathbf{W}[q] \cdot \mathbf{z}[p+q-1] + b, \tag{4}$$

where p represents the position index in the output feature map, q is the index over the kernel/filter positions, $y[p]$ denotes the output of the convolution at position p, $\mathbf{W}[q]$ is the q-th learnable weight of the convolutional kernel of size k, and $\mathbf{z}[p+q-1]$ is the corresponding element of the input latent vector $\mathbf{z}$. The index offset $p+q-1$ ensures the kernel slides across the input in a windowed fashion, and the term b is a learnable bias added to each output. To further enhance feature representation, an attention mechanism is applied to focus on the most informative temporal patterns in the convolved features. Given a feature matrix $\mathbf{H} \in \mathbb{R}^{F\times k}$, where F is the number of time steps and k is the feature dimension, attention scores $\mathbf{e}$ are computed as:

$$\mathbf{e}_i = \sigma(\mathbf{W}_a\mathbf{h}_i + \mathbf{b}_a), \tag{5}$$

where $\mathbf{h}_i \in \mathbb{R}^k$ is the feature vector at time step i, $\mathbf{W}_a \in \mathbb{R}^{v\times k}$ is the attention weight matrix, v is the dimensionality of the intermediate attention space, and $\mathbf{b}_a \in \mathbb{R}^v$ is the attention bias vector. The attention scores are then normalized using the softmax function α as:

$$\alpha_i = \frac{\exp(\mathbf{e}_i)}{\sum_{i=1}^{F}\exp(\mathbf{e}_i)}, \tag{6}$$

producing attention weights $\alpha_i \in [0, 1]$ for each time step. The final context vector $\mathbf{c} \in \mathbb{R}^k$, which aggregates the most relevant temporal information, is computed as:

$$\mathbf{c} = \sum_{i=1}^{F} \alpha_i\mathbf{h}_i. \tag{7}$$

The overall loss function $\mathcal{L}$ integrates $\mathcal{L}_{\text{recon}}$ and classification loss $\mathcal{L}_{\text{cls}}$ to achieve balanced optimization:

$$\mathcal{L} = \mathcal{L}_{\text{recon}} + \lambda\mathcal{L}_{\text{cls}}, \tag{8}$$

where $\mathcal{L}_{\text{cls}}$ is the categorical cross-entropy loss for binary classification, and λ balances the contributions of both reconstruction and classification accuracy.

B. CAENet Model Architecture

Fig. 2 illustrates the architecture of the CAENet model, which is determined through a comprehensive sequential process aimed at identifying the most effective model configuration for attack detection. We perform a grid search to determine the number of units, filter sizes, kernel functions, and other critical parameters. Through grid search and cross-validation, we arrive at the optimal architecture, beginning with DAE layers (64→32→16 units) for dimensionality reduction and reconstruction. These layer sizes are chosen to balance the reconstruction loss while retaining essential features of the data. The Conv1D layers are configured with 32 and 64 filters and a kernel size of 3 that extracts spatial and temporal features. ReLU activation and batch normalization are incorporated based on their ability to improve convergence and prevent vanishing gradients. The attention mechanism is fine-tuned to include global average pooling and dense layers (64→32 units) for prioritizing significant temporal features, while a dropout rate of 0.3 is selected to mitigate overfitting. Finally, the softmax dense layer with 2 output units optimizes to achieve the highest classification accuracy for the binary

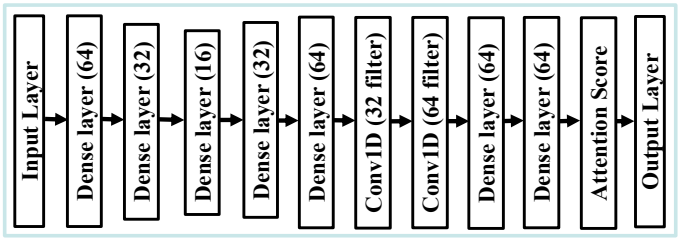

Fig. 2. Illustration of the CAENet model architecture.

classification task. This architecture reflects the outcome of extensive experimentation and optimization, ensuring that each component is tailored to maximize performance and computational efficiency for attack detection in EV charging session data.

C. Benchmark Models

To validate the effectiveness of the CAENet model, we compare it with traditional ML models, including decision trees (DT), RF, and SVM. These models are chosen for their simplicity, interpretability, and computational efficiency, serving as baseline classifiers for evaluating the performance of the deep learning approach [20]. DT classifies data by using tree-structured rules, where splits are determined based on criteria such as information gain or Gini impurity. However, they are prone to overfitting, particularly with complex datasets. To address this limitation, RF creates an ensemble of DTs trained on bootstrap samples, introducing feature randomness at each split to improve generalization and reduce overfitting. SVM, on the other hand, classifies data by constructing a hyperplane that separates classes, with the option to use kernel functions for handling non-linear separability.

D. Benchmark Model Hyperparameters

To ensure optimal performance, hyperparameter tuning is performed for all the benchmark models. For DTs, the maximum tree depth is set to 20, the minimum number of samples required to split a node is set to 5, and the minimum number of samples for a leaf node is set to 2. The number of estimators is set to 100 for RFs, and the maximum tree depth is left unlimited to allow full growth. The minimum number of samples required to split a node is set to 2, while the minimum number needed for a leaf node is set to 1. Additionally, the number of features considered for the best split is set to the square root of the total number of features. For SVM, the best performance is achieved by setting the regularization parameter to 1 and using a linear kernel. These optimized parameters enable the SVM to construct a robust decision boundary while maintaining computational efficiency.

V. Result Discussion

This section evaluates the CAENet model compared to benchmark models, including DT, RF, and SVM. While the benchmark models provide valuable context, the focus is on demonstrating the superior performance of the CAENet model in detecting CPAAs with high precision, DR, and F1 scores.

TABLE II
Detection Performance of the Investigated Models (%)

Model	Accuracy	Precision	DR	F1 Score
DT	87.10	93.60	87.02	89.22
RF	89.28	93.28	84.50	90.67
SVM	79.04	94.04	88.57	83.52
CAENet	94.47	95.02	94.47	94.45

A. Evaluation Metrics

The performance evaluation relies on four metrics: accuracy, precision, DR, and F1 score. Accuracy measures the proportion of correct classifications, including both attacks and benign samples, and is computed as:

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

Precision assesses the proportion of predicted attacks that are actual attacks:

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}.$$

The DR, also known as recall or sensitivity, evaluates the proportion of actual attacks that the model correctly identifies:

$$\text{DR} = \frac{\text{TP}}{\text{TP} + \text{FN}}.$$

The F1 score combines precision and DR into a single harmonic mean, reflecting a balance between minimizing false positives and false negatives:

$$\text{F1 Score} = 2 \cdot \frac{\text{Precision} \cdot \text{DR}}{\text{Precision} + \text{DR}}.$$

TP, TN, FP, and FN denote true positive, true negative, false positive, and false negative samples, respectively.

B. Numerical Results

Our simulation results, summarized in Table II, highlight the performance of the CAENet model compared to benchmark models. Overall, the CAENet-based detector outperforms all benchmark models across all evaluation metrics, demonstrating its ability to effectively handle the complexities of EV charging session data. The results are analyzes as follows.

- With an accuracy of 94.47%, CAENet surpasses SVM, DT, and RF by 19.52%, 8.46%, and 5.81%, respectively. Such an improvement highlights superior capacity of CAENet to model intricate temporal and spatial interactions, whereas benchmark models rely on static data representations and require substantial manual feature engineering to capture time dependent trends and spatial correlations.
- In terms of precision, CAENet achieves 95.02%, with improvements of 1.04%, 1.52%, and 1.87% over SVM, DT, and RF, respectively. Such a performance underscores

the reliability of CAENet in accurately identifying positive instances while effectively minimizing false positives.

- CAENet offers a DR of 94.47%, which marks a significant leap over the benchmark models, outperforming SVM, DT, and RF by 6.65%, 8.56%, and 11.81%, respectively. Such a high DR reflects the ability CAENet to reduce false negatives, ensuring robust detection of critical instances. Such high DR is particularly crucial in EV charging session data, where missed detections can lead to SG instability.
- CAENet achieves the highest F1-Score of 94.45%, balancing precision and DR effectively, surpassing SVM, DT, and RF by 13.09%, 5.86%, and 4.17%, respectively.

Such a superior performance across all metrics underscores CAENet as the a robust and reliable model for detecting attacks in EV charging session data.

VI. Conclusions

The integration of EVCSs into SGs demands robust attack detection to counter vulnerabilities like CPAAs. This study introduced CAENet, combining DAE, CNN, and attention mechanisms to detect CPAAs effectively. CAENet achieved a DR of 94%, surpassing benchmark machine learning models like SVM, DT, and RF by $7 - 12\%$. Such a high DR underscored the ability of the CAENet-based detector to reduce false negatives, ensuring robust identification of CPAAs and significantly enhancing the stability of smart grid operations. Future work will integrate graph neural networks to better model spatiotemporal patterns, enhancing attack detection in smart city infrastructures.

References

[1] P. W. Pong *et al.*, "Cyber-enabled grids: Shaping future energy systems," *Advances in Applied Energy*, vol. 1, p. 100003, Dec. 2021.

[2] M. ElKashlan *et al.*, "A machine learning-based intrusion detection system for iot electric vehicle charging stations (evcss)," *Electronics*, vol. 12, no. 4, Feb. 2023.

[3] A. A. Shafee *et al.*, "Detection of distributed denial of charge (ddoc) attacks using deep neural networks with vector embedding," *IEEE Access*, vol. 11, pp. 75 381–75 397, Jan. 2023.

[4] S. R. Fahim *et al.*, "Graph autoencoder-based power attacks detection for resilient electrified transportation systems," *IEEE Transactions on Transportation Electrification*, vol. 10, no. 4, pp. 9539–9553, Dec. 2024.

[5] A. Takiddin *et al.*, "Spatio-temporal graph-based generation and detection of adversarial false data injection evasion attacks in smart grids," *IEEE Transactions on Artificial Intelligence*, vol. 5, no. 12, pp. 6601–6616, Dec. 2024.

[6] D. Said *et al.*, "Cyber-attack on p2p energy transaction between connected electric vehicles: A false data injection detection based machine learning model," *IEEE Access*, vol. 10, pp. 63 640–63 647, Jun. 2022.

[7] A. Akbarian *et al.*, "Detection of cyber attacks to mitigate their impacts on the manipulated ev charging prices," *IEEE Transactions on Transportation Electrification*, vol. 10, no. 4, pp. 8881–8892, Dec. 2024.

[8] H. Jahangir *et al.*, "Charge manipulation attacks against smart electric vehicle charging stations and deep learning-based detection mechanisms," *IEEE Transactions on Smart Grid*, vol. 15, no. 5, pp. 5182–5194, Sept. 2024.

[9] A. M. Abu-Nassar *et al.*, "Early detection of cyber-physical attacks on electric vehicles fast charging stations using wavelets and deep learning," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 2, pp. 220–231, Jan. 2024.

[10] A. Hussain *et al.*, "Anomaly detection using bi-directional long short-term memory networks for cyber-physical electric vehicle charging stations," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 2, pp. 508–518, Aug. 2024.

[11] I. Benfarhat *et al.*, "Temporal convolutional network approach to secure open charge point protocol (ocpp) in electric vehicle charging," *IEEE Access*, vol. 13, pp. 15 272–15 289, Jan. 2025.

[12] M. Nabil *et al.*, "Deep recurrent electricity theft detection in ami networks with evolutionary hyper-parameter tuning," in *International Conference on Internet of Things (iThings)*. Atlanta, GA, USA, 14-17 Jul. 2019, pp. 1002–1008.

[13] A. Takiddin *et al.*, "Variational auto-encoder-based detection of electricity stealth cyber-attacks in ami networks," in *28th European Signal Processing Conference (EUSIPCO)*. Amsterdam, Netherlands, 8-21 Jan. 2020, pp. 1590–1594.

[14] Pamir *et al.*, "Non-technical losses detection using autoencoder and bidirectional gated recurrent unit to secure smart grids," *IEEE Access*, vol. 10, pp. 56 863–56 875, Apr. 2022.

[15] A. Takiddin *et al.*, "Deep autoencoder-based anomaly detection of electricity theft cyberattacks in smart grids," *IEEE Systems Journal*, vol. 16, no. 3, pp. 4106–4117, Jan. 2022.

[16] M. Bharathidasan *et al.*, "A review on electric vehicle: Technologies, energy trading, and cyber security," *Energy Reports*, vol. 8, pp. 9662–9685, Aug. 2022.

[17] Z. J. Lee *et al.*, "ACN-Data: Analysis and Applications of an Open EV Charging Dataset," in *Proceedings of the Tenth International Conference on Future Energy Systems*. Phoenix, Arizona, Jun. 2019.

[18] M. R. Ahasan *et al.*, "Benchmarking unsupervised machine learning for mobile network anomaly detection," in *International Conference on Innovations in Science, Engineering and Technology (ICISET)*. Chittagong, Bangladesh, 26-27 February 2022, pp. 468–473.

[19] H. He *et al.*, "Adasyn: Adaptive synthetic sampling approach for imbalanced learning," in *IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence)*. Hong Kong, China, 01-08, Jun. 2008, pp. 1322–1328.

[20] M. R. Ahasan *et al.*, "Supervised learning based mobile network anomaly detection from key performance indicator (kpi) data," in *IEEE Region 10 Symposium (TENSYMP)*. Mumbai, India,, 01-03 Jul. 2022, pp. 1–6.