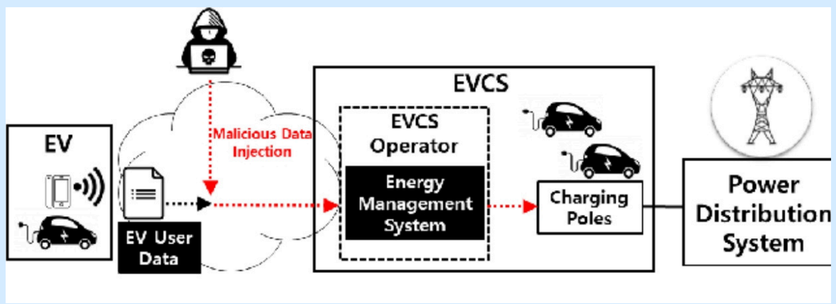
Secure EVCS: Cyber-Physical Attack Detection for EV Charging Infrastructure

Sofia Tenghoff and Md. Rakibul Ahasan

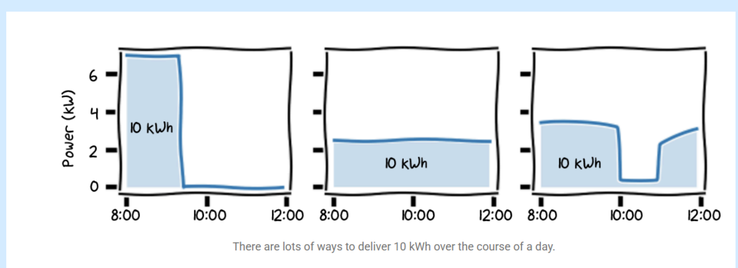
Introduction

As electric vehicles (EVs) become more common, the need for secure and efficient electric vehicle charging stations (EVCSs) increases. When integrated with smart grid (SG) technology, EVCSs become vital components of smart city infrastructure. However, EVCSs are often subject to cyberattacks, such as manipulations of charging parameters like start time, energy demand, and charging duration by malicious actors. This research project investigates which machine learning (ML) model performs best at detecting cyberattacks in EVCSs. Performance is measured in terms of detection rate (DR). The tested ML models include decision tree (DT), random forest (RF) support vector machines (SVM), and feed forward neural networks (FNN) The purpose of this research is to save EVCS owners time and money and to protect electric vehicle drivers' data privacy. The methodology involved analyzing data from the ACN website, writing code that builds ML models, and training and testing those models on the data. The results show FNN as the model yielding the best DR.

Types of Cyber Attack

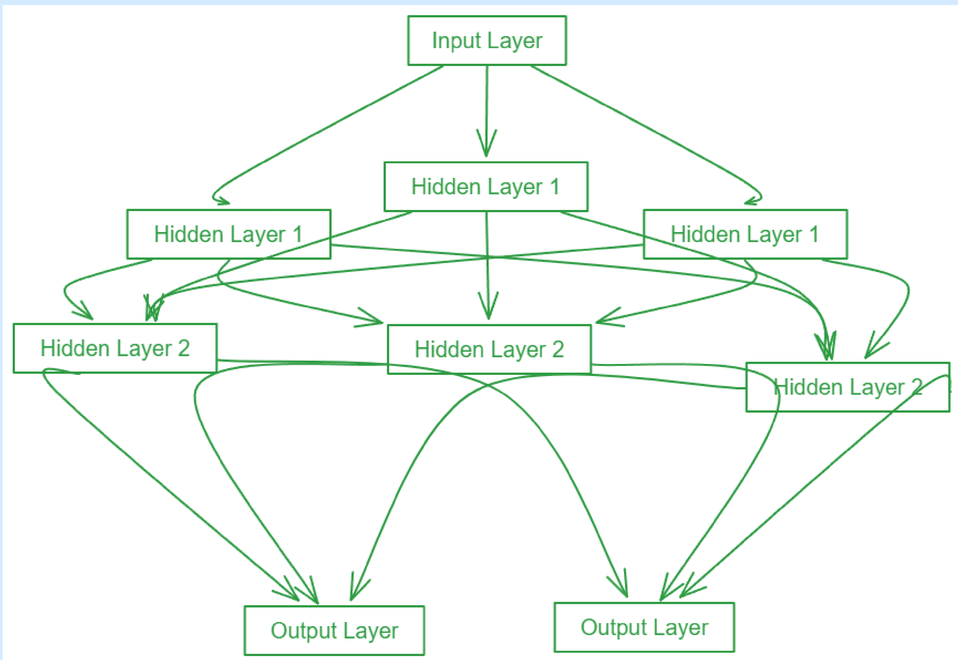


EVCS charging profile manipulation attack

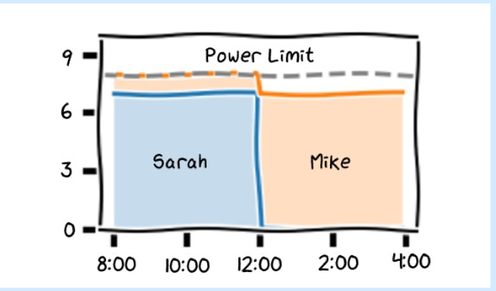


Change in energy demand

FNN Architecture



Cyber Attack Cont....



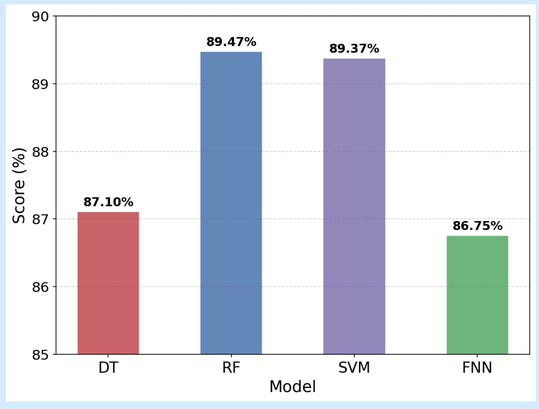
Charging start and end times in relation to energy demand

Methodology

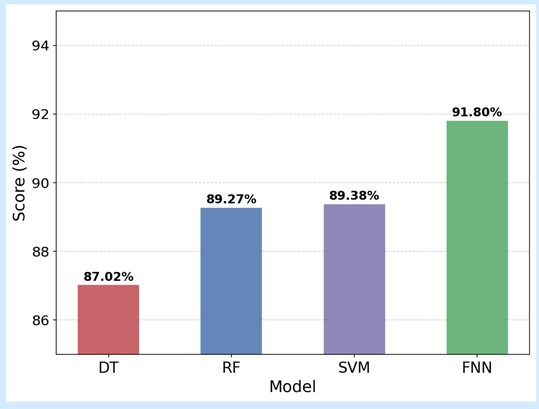
- Collect EVCS charging session data from ACN website
- JSON file is collected
- Convert the JSON file into CSV file using Python.
- Extract cyber features.
- Use 80% of dataset as training set
- Use 20% of dataset as testing set
- Build the machine learning model
- Collect accuracy, recall (detection rate), precision, and F1-Score value
- Perform analysis on the generated results

Results

Accuracy



Detection Rate



Evaluation Metrics

ACTUAL VALUES	POSITIVE	NEGATIVE
POSITIVE	TP	FN
NEGATIVE	FP	TN

$$Precision = \frac{TP}{TP + FP} \qquad Recall = \frac{TP}{TP + FN}$$

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

$$F1\ Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Discussion

Our initial research question was out of SVM, FNN, DT, and RF, which machine learning model can predict cyberattacks on EVCS with the greatest recall? We also measured accuracy, seen in the bar charts above. So far, FNN surpasses SVM, DT, and RF in terms of recall. SVM achieved a recall of 89.38%, DT achieved a recall of 87.02%, and RF achieved a recall of 89.27%, while FNN achieved a recall of 91.8%. This matters because recall is the rate of all positives in a dataset that are detected. For cyberattacks, this is very important because it's better to detect all attacks and some extra, which would just be overly cautious, than to miss some attacks and thus cost a company thousands of dollars. The prevailing of FNNs over SVMs, DTs, and RFs points to the consistent superiority of deep ML models over shallow models.

References

[1] M. R. Ahasan, S. R. Fahim and A. Takiddin, "Securing EVCS Infrastructure Against Cyberattacks with a Deep Learning-Based Detection Model," 2025 10th International Conference on Fog and Mobile Edge Computing (FMEC), Tampa, FL, USA, 2025, pp. 33-38.

[2] S. R. Fahim et al., "Graph Autoencoder-Based Power Attacks Detection for Resilient Electrified Transportation Systems," in IEEE Transactions on Transportation Electrification, vol. 10, no. 4, pp. 9539-9553, Dec. 2024.

[3] M. R. Ahasan, S. Rahman Fahim, R. Atat and A. Takiddin, "A Graph-Based Optimization Approach for Resilient EV Rerouting in Disrupted Charging Networks," 2026 IEEE 23rd Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2026,

[4] https://tinyurl.com/FNNNew