

Phase 2 – Data Mining for Cybersecurity

Introduction

Electric Vehicle Supply Equipment (EVSE) is a critical component of modern smart transportation systems. Due to continuous connectivity with vehicles, local management systems, and remote cloud services, EVSE systems are exposed to various cyber threats. This project applies data mining techniques to detect cyberattacks using the CICEVSE2024 dataset.

Data Pre-processing

The datasets were preprocessed to ensure quality and consistency. Missing values were checked, numerical features were scaled, and labels were encoded. Feature selection was applied to reduce noise and improve model performance.

Exploratory Data Analysis (EDA)

EDA was conducted to analyze behavioral differences between benign and attack scenarios. Power consumption and host events showed clear deviations during attack conditions compared to normal operation.

Data Mining Technique and Application

Supervised classification using Random Forest was selected due to labeled data availability. The dataset was split into training and testing sets, and evaluation metrics such as accuracy, precision, recall, and F1-score were used.

Conclusion

The results demonstrate that data mining techniques are effective in detecting cyber threats in EVSE environments. Host-based features provided strong detection for stealth attacks, while power data detected resource-intensive attacks.

References

CICEVSE2024 Dataset, Canadian Institute for Cybersecurity.