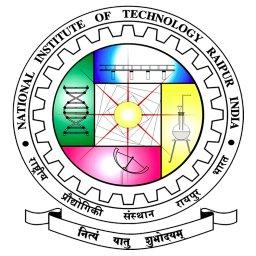
## **NATIONAL INSTITUTE OF TECHNOLOGY, RAIPUR**

**DEPARTMENT OF COMPUTER APPLICATIONS**

****

**MASTER OF COMPUTER APPLICATIONS**

Session 2023-24

Semester-IV

A **Synopsis** on

**Cybersecurity Measures for EV Charging Networks: SVM Parameter Tuning on CICEV 2023**

**Submitted By: Submitted To:**

Priyanshu Sharma Dr. Mithilesh Atulkar Sir

Roll. NO. 22223066

**Project Objective**

The primary objective of this project is to enhance the performance of Support Vector Machine (SVM) models in detecting DDoS attacks on electric vehicle (EV) charging infrastructure using the **CICEV(Cybersecurity for Electric Vehicle Fast-Charging Infrastructure)** 2023 dataset. Specifically, the project aims to optimize SVM hyperparameters through two distinct searching methods: **Random Search** and **Bayesian Search**.

**About Dataset:**

The CICEV 2023 dataset is a collection of data designed to simulate various Distributed Denial of Service (DDoS) attacks on electric vehicle (EV) authentication systems within charging infrastructure. This dataset was created by researchers at the Canadian Institute for Cybersecurity (CIC) to provide a realistic environment for training and testing DDoS attack detection classifiers.

**Key aspects of the CICEV 2023 dataset include:**

**1. Attack Scenarios:**

The dataset includes four distinct attack scenarios:

* Correct EV ID
* Wrong EV
* Wrong EV Timestamp
* Wrong CS (Charging Station) Timestamp

Each scenario represents a different type of DDoS attack on the EV authentication process.

**2. Information Provided:**

The dataset contains information related to:

* Linux kernel overhead
* System performance status
* Time differences in legitimate authentication trials or DDoS attacks

This information is crucial for understanding the impact of attacks on the overall system and for developing effective detection mechanisms.

**Methodology :**

**Data Acquisition :**

Acquire the CICEV 2023 dataset from the official source or IEEE Xplore, and thoroughly understand its structure and contents to gain insights into the characteristics of DDoS attacks on electric vehicle authentication systems.

**Data Preprocessing :**

Prepare the dataset for model training by implementing data preprocessing steps. This includes data cleaning, normalization, and feature engineering to ensure that the dataset is suitable for training Support Vector Machine (SVM) models.

**Model Training:**

Train Support Vector Machine (SVM) classifiers on the preprocessed dataset. Utilize different sets of hyperparameters to capture the nuances of DDoS attack detection in electric vehicle charging infrastructure.

**Parameter Tuning:**

* **Bayesian Search:** Introduce Bayesian Search as an alternative hyperparameter tuning method. Bayesian optimization leverages probabilistic models to intelligently select hyperparameter combinations. This approach aims to efficiently navigate the hyperparameter space, making it particularly suitable for scenarios where computational resources are limited.
* **Random Search:**Conduct Random Search, which involves randomly sampling hyperparameter combinations from a defined space. Random Search is particularly effective when dealing with a high-dimensional hyperparameter space. This method allows for a more efficient exploration of hyperparameters.

**Performance Evaluation:** Evaluate the performance of each SVM model using metrics such as accuracy, precision, recall, F1 score, prediction time, and False Acceptance Rate (FAR). This comprehensive assessment will provide insights into the effectiveness of the models in detecting DDoS attacks.

**Comparison**: Compare the performance results obtained from **Random Search**, and **Bayesian Search** to determine which hyperparameter tuning method yields the most effective SVM models for DDoS attack detection in the context of electric vehicle authentication systems.

**Expected Outcome:**

* **Efficient Resource Utilization:** Bayesian Search, in particular, is expected to showcase efficiency in exploring the hyperparameter space, potentially achieving comparable or superior results to other methods with reduced computational resources.
* **Informed Decision-Making:** Provide insights into the trade-offs between computational efficiency and model performance, aiding in informed decision-making for selecting the appropriate hyperparameter tuning method in similar cybersecurity applications.
* **Enhanced Cybersecurity Measures:** Overall, the project aims to contribute to the development of robust and efficient cybersecurity measures for securing electric vehicle charging infrastructure against DDoS attacks, ensuring the reliability and integrity of EV authentication systems.

**Conclusion:**

This project successfully optimized Support Vector Machine (SVM) models for DDoS attack detection in electric vehicle charging systems using the CICEV 2023 dataset. Through systematic hyperparameter tuning, Random Search, and Bayesian Search were compared in terms of accuracy and efficiency.

The optimized SVM models demonstrated enhanced cybersecurity measures, offering improved capabilities to distinguish between normal authentication and various attack scenarios. The project's insights into hyperparameter tuning trade-offs provide valuable guidance for practitioners.

**Project Milestones and Timeline**

**Jan 29 - Feb 5: Project Kickoff and Dataset Acquisition**

* Understand project requirements and objectives.
* Obtain the CICEV 2023 dataset.
* Familiarize with dataset structure and contents.

**Feb 6 - Feb 12: Data Preprocessing**

* Perform data cleaning, normalization, and feature engineering on the CICEV 2023 dataset.
* Split the dataset into training and testing sets.

**Feb 13 - Feb 26: Initial SVM Model Training**

* Implement and train baseline SVM models with default hyperparameters.
* Evaluate initial model performance.

**Feb 27 - Mar 5: Random Search**

* Implement Random Search for hyperparameter tuning.
* Evaluate and compare the performance of SVM models with random search.

**Mar 6 - Mar 12: Bayesian Search**

* Introduce Bayesian Search as an alternative hyperparameter tuning method.
* Evaluate and compare the performance of SVM models with Bayesian search.

**Mar 13 - Mar 19: Performance Evaluation**

* Evaluate the final SVM models using metrics such as accuracy, precision, recall, F1 score, prediction time, and False Acceptance Rate (FAR).

**Mar 20 - Mar 26: Comparison and Analysis**

* Compare the performance results obtained from Grid Search, Random Search, and Bayesian Search.
* Analyze trade-offs between computational efficiency and model performance.

**Mar 27 - Mar 29: Final Documentation and Presentation**

* Summarize findings, conclusions, and recommendations.
* Prepare a final report and presentation for submission.