**MODULES**

**Data Preprocessing Module:** This module focuses on preparing and refining the input data for the machine learning algorithms. It involves tasks such as data cleaning, handling missing values, normalization, and transforming the raw data from the Aposemat IoT-23 dataset into a format suitable for effective learning by the algorithms.

**Machine Learning Algorithm Implementation Module:** This module encompasses the implementation of machine learning algorithms, including Decision Tree, Random Forest, and Naive Bayes. Each algorithm is configured and trained on the preprocessed data to learn and recognize patterns indicative of IoT network attacks.

**Dataset Integration Module:** The system integrates multiple labeled datasets beyond the Aposemat IoT-23 dataset to ensure a more comprehensive understanding of diverse attack patterns. This module facilitates the combination of various datasets, promoting a broader and more adaptable detection capability.

**Dynamic Model Adaptation Module:** To address the dynamic nature of IoT threats, this module introduces dynamic and adaptive machine learning models. These models continuously evolve and learn from ongoing network behaviors, allowing the system to adapt to emerging threats in real-time and enhance its ability to detect novel attack patterns.

**Scalability and Optimization Module:** This module focuses on enhancing the scalability and efficiency of the system. It includes strategies for accommodating large-scale IoT networks, optimizing resource utilization, and incorporating lightweight algorithms suitable for deployment on resource-constrained IoT devices. The goal is to ensure the system performs effectively across diverse network environments while efficiently managing computational resources.

Top of Form