**Cyber net: detection of cyber-attacks in network using machine learning techniques**

**ABSTRACT**

In today's interconnected world, the widespread adoption of Internet of Things (IoT) devices has brought forth a host of conveniences and opportunities. However, this technological revolution has also opened the door to a new breed of cyber threats, with attackers exploiting vulnerabilities in IoT devices to compromise user privacy, disrupt critical services, and wreak havoc. Traditional security measures have proven inadequate to combat the evolving complexity of these cyber-attacks, necessitating a more advanced and adaptive approach. This urgency has given rise to the development of a Machine Learning Model for Cyber Attack Detection and Classification in IoT Environments (ML-IoT-CD). In addition, the need for a robust cybersecurity solution in IoT environments has become paramount due to the increasing reliance on these devices for critical applications. Existing intrusion detection systems and conventional security measures often lack the scalability and agility needed to keep pace with rapidly evolving attack techniques. As a result, there is a pressing demand for an intelligent, automated, and proactive cyber defense mechanism capable of real-time detection and classification of emerging cyber threats. The ML-IoT-CD model aims to fulfill this need by harnessing the power of machine learning algorithms to analyze vast amounts of data generated by IoT devices. By doing so, it can effectively distinguish between legitimate and malicious activities, thereby bolstering the security posture of IoT ecosystems.

**Project Outcomes, Existing System & Drawbacks, Proposed System & Advantages.**

**Project Outcomes**

The project successfully implements a **Machine Learning-based Cyber Attack Detection System** for IoT environments. The key outcomes include:

* **Improved Accuracy**: The Random Forest Classifier (RFC) model provides better accuracy in detecting cyber threats compared to traditional models.
* **Scalability**: The system is designed to handle large-scale IoT deployments effectively.
* **Real-time Detection**: The model can analyze network traffic in real-time and classify threats accurately.
* **Feature Optimization**: The feature selection method reduces processing resource demand, making it suitable for resource-constrained IoT devices.

### ****Existing System & Drawbacks****

#### ****Existing System****

* Uses **Logistic Regression** for cyber-attack detection.
* Based on statistical models to classify network traffic as normal or attack.
* Implements **signature-based** and **anomaly-based** Intrusion Detection Systems (IDS).

#### ****Drawbacks****

* **Limited Detection Capability**: Signature-based methods struggle to detect new or unknown attacks.
* **High False Positives**: Anomaly detection models sometimes classify legitimate traffic as attacks.
* **Resource Constraints**: Many IoT devices lack the computational power to run complex security models.
* **Scalability Issues**: Traditional methods fail to handle large volumes of IoT data efficiently.

### ****Proposed System & Advantages****

#### ****Proposed System****

* Uses **Machine Learning (ML) techniques**, specifically the **Random Forest Classifier (RFC)**.
* **Data Preprocessing** with **Standard Scaling** to enhance detection efficiency.
* **Feature Engineering** to select the most relevant network traffic features.
* **Training & Testing on UNSW-NB15 Dataset** for accurate cyber-attack classification.

#### ****Advantages****

* **Higher Detection Accuracy**: RFC performs better than Logistic Regression in classifying attack categories.
* **Adaptive to New Threats**: The model can detect previously unseen attacks (zero-day threats).
* **Resource Optimization**: Feature selection reduces processing requirements, making it more IoT-friendly.
* **Scalability & Real-Time Processing**: Can analyze large datasets efficiently.
* **Robustness Against Evolving Threats**: The system updates itself with new attack patterns using ML techniques.

This system enhances **IoT cybersecurity** by providing an **intelligent, scalable, and automated attack detection solution**.