DETECTION OF IOT CYBER ATTACK USING MACHINE LEARNING

Internet of Things (IoT) is a new paradigm that integrates the Internet and physical objects belonging to different domains such as home automation, industrial process, human health and environmental monitoring. The number of IoT devices is expected to reach 50 Billion by 2023. Various smart city applications connect enormous loT devices to real-world objects, which indeed have very important benefits to urban life. However, the massive number of loT devices over heterogeneous variety types of services, technologies, devices, and protocols (e.g. Wireless, Wired, Satellite, Cellular, Bluetooth, etc.) leads to the complexity of managing future IoT networks. Therefore, the network traffic of a smart city via loT systems is growing exponentially and introducing new cyber security challenges since these loT devices are being connected to sensors that are directly connected to massive cloud servers .These cyber threats can obtain unauthorized access to the loT devices without the knowledge of either the eligible user or administrator. In order to mitigate these cyber attacks, the developers need to enhance new techniques for detecting infected loT devices.

Cyber Security on IoT introduces some significant challenges:

- Data collected are very sensitive. Most of the times they capture personal data and/or business critical data. Privacy is very important
- Each device generates data at scale. But the device has constraints on memory, computation and battery life. Connecting each device to the cloud reduces the life of the device.

This calls for a new paradigm in Machine Learning that exhibits the following features:

- Data should not be moved out of the device and/or network
- The Machine Learning models should be privacy-preserving

The machine learning algorithms can be used are Logistic Regression (LR), Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF), and Artificial Neural Network (ANN). Anomaly detection is the identification of rare items, events or observations which raise suspicions by differing significantly from the majority of the data. Anomaly detection is a class of unsupervised machine learning models that identifies anomalies in network data. In cyber security, anomalies are flagged as a potential threat. To address the loT cyber security threats in a smart city, we propose an Anomaly Detection loT (AD-IoT) system, which is an intelligent anomaly detection based on Random Forest machine learning algorithm. The proposed solution can effectively detect compromised loT devices at distributed fog nodes.