كلية الحاسبات وتقنية المعلومات
FACULTY OF COMPUTING
& INFORMATION TECHNOLOGY

الماجستير المهني في الذكاء الاصطناعي
Professional Master in
Artificial Intelligence

Project Proposal

IoT Sentinel: Intelligent Detection of Cyber Threats in Smart Devices

Supervisor:
Dr. Sultanah Alshamari

Problem Statement:

In recent years, the number of IoT devices has increased dramatically, connecting everything from home cameras and smart TVs to healthcare and industrial systems. However, most of these devices were not designed with strong security in mind, which makes them easy targets for cyberattacks. Many of them send and receive large amounts of data continuously, and any abnormal behavior in this traffic could indicate a potential threat.

The main problem is that traditional security tools are not efficient at recognizing new or unknown attack patterns, especially in large IoT environments. Therefore, there is a real need for an intelligent system that can automatically detect unusual network behaviors and identify cyber threats before they cause harm.

Objective:

The main goal of this project is to develop an intelligent system that can detect abnormal behaviors in IoT network traffic using machine learning techniques. By analyzing real network data from different IoT devices, the system aims to distinguish between normal and malicious activities automatically.

This approach will help improve the detection of unknown or emerging attacks that traditional methods often miss. In the end, the goal is to support IoT security by providing faster and more accurate detection of potential cyber threats, reducing the risk of damage or data loss.

Dataset Information:

- Name of the dataset: CIC IoT 2023
- Source of Dataset: https://www.kaggle.com/datasets/akashdogra/cic-iot-2023/data
- Dataset description:
  This dataset contains real network traffic collected from various Internet of Things (IoT) devices operating under both normal and attack conditions. Each record represents one network flow between devices and includes around 47 features such as protocol type, flow duration, packet rate, header length, and TCP flag indicators. The dataset also includes labeled samples of multiple cyberattacks, including DDoS, DoS, and Mirai botnet traffic, as well as normal behavior.
- Relevance to the Project:
  This dataset is closely related to the project's goal of detecting abnormal IoT behavior using AI-based techniques. It provides realistic and labeled network data that capture both normal and malicious activities, which allows the model to learn meaningful traffic patterns. The variety of attack types in the dataset makes it highly suitable for training and testing an intelligent system capable of identifying cyber threats in IoT environments.