Improving the security of IoT devices

Compiling a dataset with IoT traffic data to detect traffic malware and anomalies for IoT devices

TTKOM achieved this using
• SAS® Viya® in Microsoft Azure • SAS® Studio

SAS Hackathon 2023 • Telecom Track

Challenge

The number of devices connected to the Internet of Things (IoT) has increased rapidly in the last five years.

- These devices are now used for a wide range of applications in homes and businesses around the world.
- However, these devices are capable of collecting and transmitting sensitive data.
- They are therefore a potential target for cyber-attackers, and there are very real concerns about their security.

Innovation

This solution aimed to use machine learning models to predict whether network traffic contains any anomalies that might be associated with malign intentions.

TTKOM:

- Used the IoT23 dataset to supply data from devices.
- In a controlled environment, simulated various types of network attacks to train several models to predict whether network traffic is benign or malicious.
- Deployed the best model in a real-world scenario to predict malicious network traffic.

Impact

The model should help to improve the security of IoT devices by accurately predicting malicious network traffic.

- It should help to prevent cyber attacks on IoT devices and networks.
- The model could be used across telecoms networks and other networks connected to IoT devices.
- It may also help to increase awareness of the vulnerabilities of IoT systems and devices.

> “IoT devices are everywhere, from our homes and workplaces to our cars and even our bodies.”
>
> Uğur Barış Öztürk • TTKOM Team