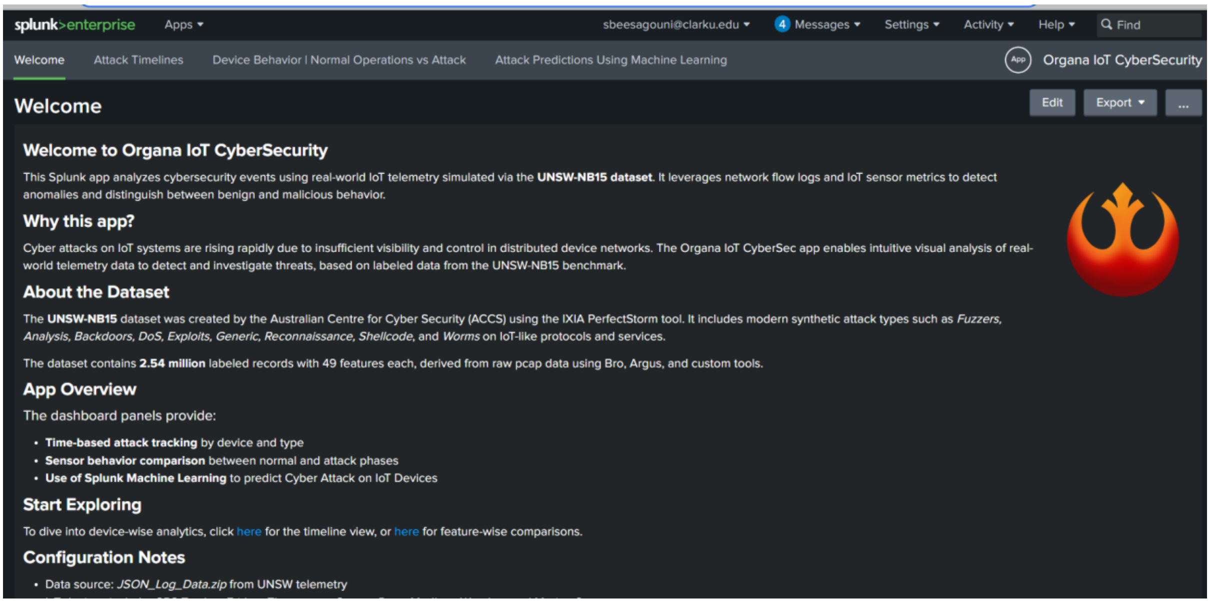
Splunk Final project

IoT Cyber Security

App url: Welcome | Splunk 9.1.0.2

App figures:



Welcome

Welcome to Organa IoT CyberSecurity

This Splunk app analyzes cybersecurity events using real-world IoT telemetry simulated via the **UNSW-NB15 dataset**. It leverages network flow logs and IoT sensor metrics to detect anomalies and distinguish between benign and malicious behavior.

Why this app?

Cyber attacks on IoT systems are rising rapidly due to insufficient visibility and control in distributed device networks. The Organa IoT CyberSec app enables intuitive visual analysis of real-world telemetry data to detect and investigate threats, based on labeled data from the UNSW-NB15 benchmark.

About the Dataset

The **UNSW-NB15** dataset was created by the Australian Centre for Cyber Security (ACCS) using the IXIA PerfectStorm tool. It includes modern synthetic attack types such as *Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode*, and *Worms* on IoT-like protocols and services.

The dataset contains **2.54 million** labeled records with 49 features each, derived from raw pcap data using Bro, Argus, and custom tools.

App Overview

The dashboard panels provide:

- **Time-based attack tracking** by device and type
- **Sensor behavior comparison** between normal and attack phases
- **Use of Splunk Machine Learning** to predict Cyber Attack on IoT Devices

Start Exploring

To dive into device-wise analytics, click here for the timeline view, or here for feature-wise comparisons.

Configuration Notes

- Data source: *JSON_Log_Data.zip* from UNSW telemetry

INTRODUCTION

This Splunk app analyzes cybersecurity events using real-world IoT telemetry simulated via the **UNSW-NB15 dataset**. It leverages network flow logs and IoT sensor metrics to detect anomalies and distinguish between benign and malicious behavior.

Why this app?

Cyber attacks on IoT systems are rising rapidly due to insufficient visibility and control in distributed device networks. The Organa IoT CyberSec app enables intuitive visual analysis of real-world telemetry data to detect and investigate threats, based on labeled data from the UNSW-NB15 benchmark.

About the Dataset

The **UNSW-NB15** dataset was created by the Australian Centre for Cyber Security (ACCS) using the IXIA PerfectStorm tool. It includes modern synthetic attack types such as *Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode*, and *Worms* on IoT-like protocols and services.

The dataset contains **2.54 million** labeled records with 49 features each, derived from raw pcap data using Bro, Argus, and custom tools.

App Overview

The dashboard panels provide:

- **Time-based attack tracking** by device and type
- **Sensor behavior comparison** between normal and attack phases
- **Use of Splunk Machine Learning** to predict Cyber Attack on IoT Devices

Start Exploring

To dive into device-wise analytics, click here for the timeline view, or here for feature-wise comparisons.

Configuration Notes

- Data source: *JSON_Log_Data.zip* from UNSW telemetry
- IoT devices include: GPS Tracker, Fridge, Thermostat, Garage Door, Modbus, Weather, and Motion Sensor
- All logs include label and type fields for supervised detection

References

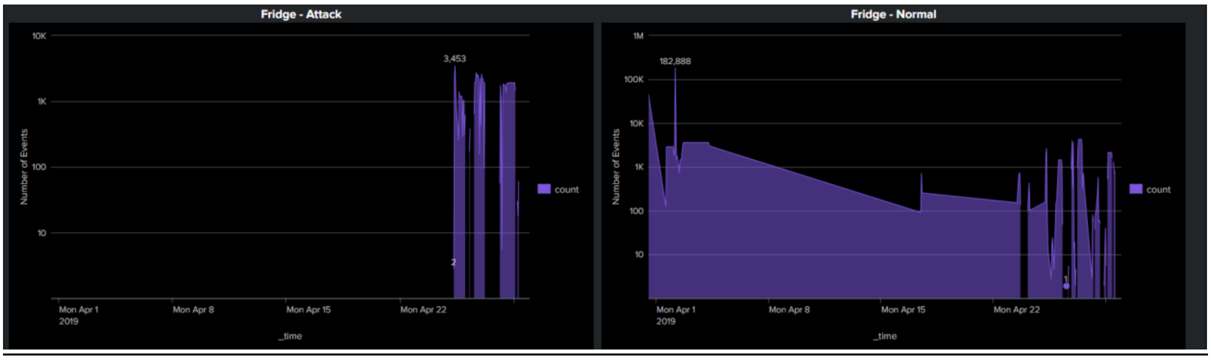
Moustafa, Nour, and Jill Slay. "*UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)*." Read the paper here.

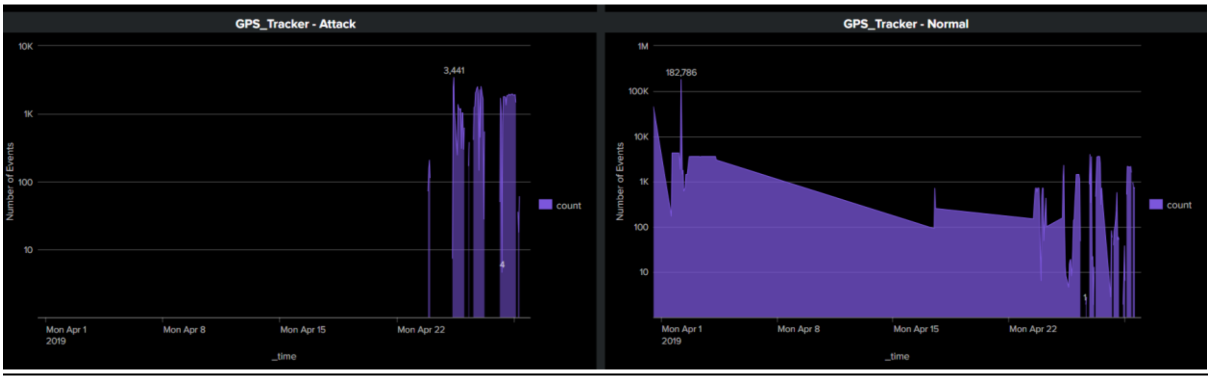
VISUALIZATIONS

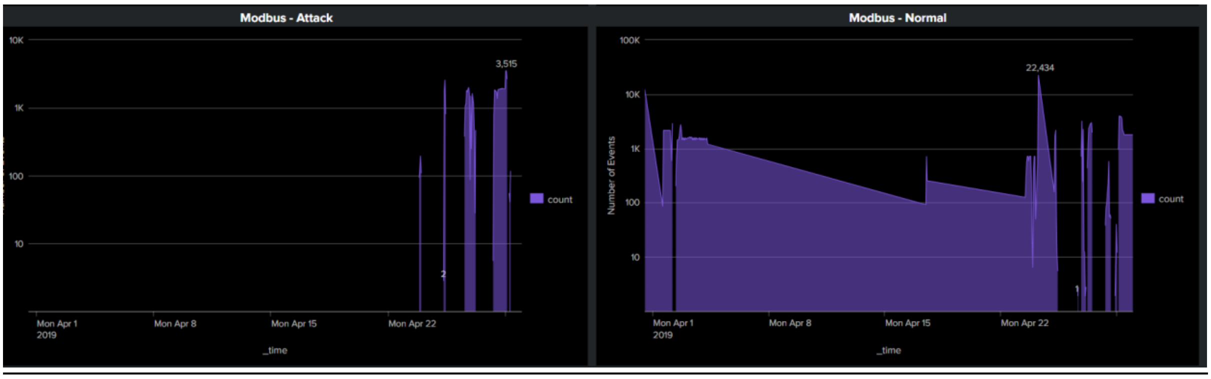
Attack Timelines:

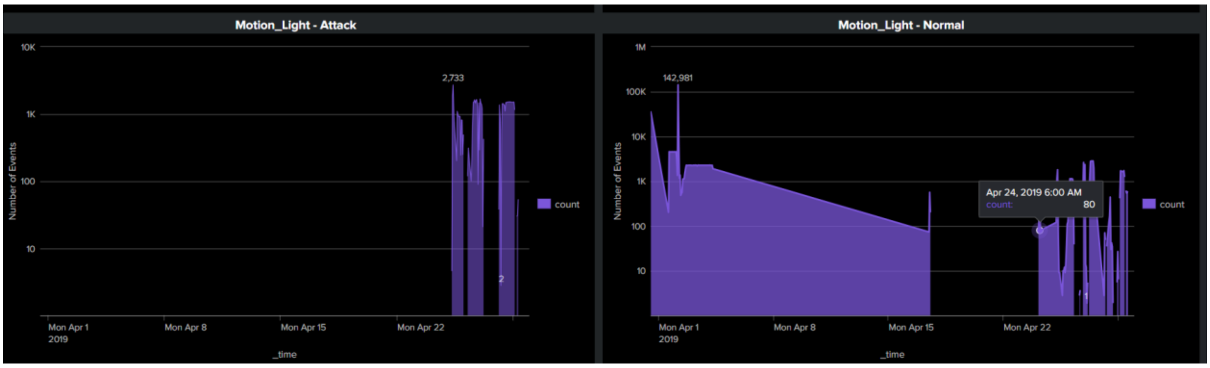
Here, we monitor seven devices - Fridge, GPS Tracker, Garage Door, Modbus controller, Motion Light, Thermostat, and Weather Station - each shown with two side-by-side graphs: "Attack" on the left and "Normal" on the right. The X-axis spans April 1-30, 2019, and the Y-axis is a log scale of event counts, letting us see both small fluctuations and massive spikes on one chart.

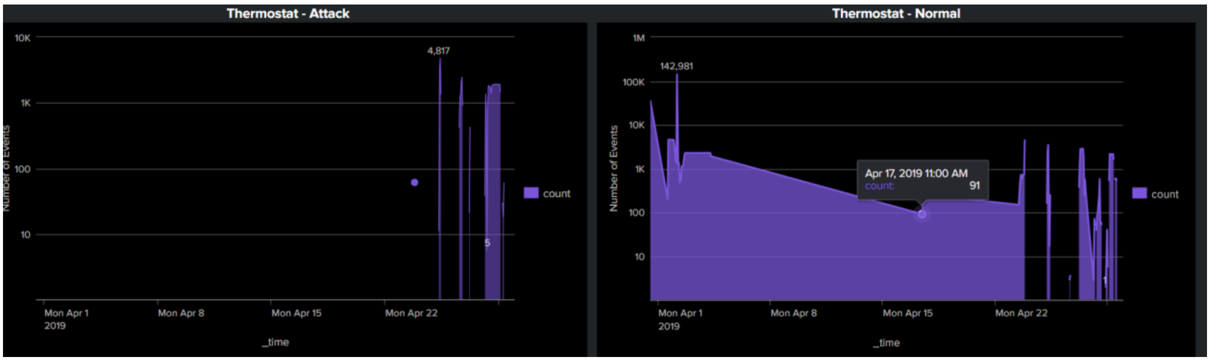
- Attack Graphs: Purple bars appear only when malicious events occur. Most days are flat at zero, with sudden spikes in late April.
- Normal Graphs: Filled purple areas show routine activity - high volume at month-start tapering off gradually. Daily usage patterns form a smooth slope rather than abrupt jumps.
- Normal activity never shows these sudden jumps - its gradual decline reflects expected device behavior.
- Spikes in attack graphs align across devices, whereas normal peaks do not synchronize

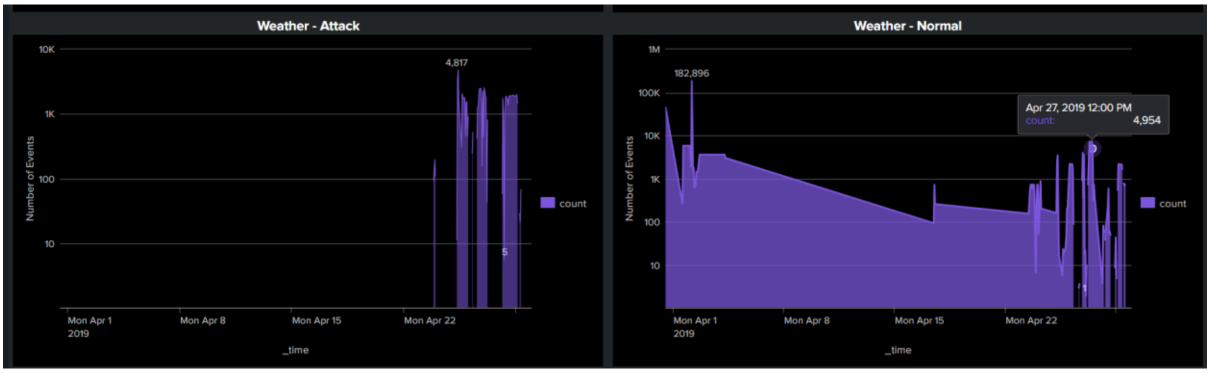

Fridge - Attack
10K
1K
100
10
Number of Events
3,453
2
count
Mon Apr 1
2019
Mon Apr 8
Mon Apr 15
Mon Apr 22
_time
Fridge - Normal
1M
100K
10K
1K
100
10
Number of Events
182,888
1
count
Mon Apr 1
2019
Mon Apr 8
Mon Apr 15
Mon Apr 22
_time


GPS_Tracker - Attack
10K
1K
100
10
Number of Events
3,441
4
count
Mon Apr 1
2019
Mon Apr 8
Mon Apr 15
Mon Apr 22
_time
GPS_Tracker - Normal
1M
100K
10K
1K
100
10
Number of Events
182,786
1
count
Mon Apr 1
2019
Mon Apr 8
Mon Apr 15
Mon Apr 22
_time


Modbus - Attack
10K
1K
100
10
3,515
2
count
Mon Apr 1
2019
Mon Apr 8
Mon Apr 15
Mon Apr 22
_time
Modbus - Normal
100K
10K
1K
100
10
Number of Events
22,434
1
count
Mon Apr 1
2019
Mon Apr 8
Mon Apr 15
Mon Apr 22
_time







Why It Matters

- Rapid Detection: Those jagged bars instantly flag "something's wrong" in late April - no need to go through millions of logs.
- Incident Mapping: Synchronized spikes across devices point to a single campaign, helping us trace the attacker's path and timing.
- Impact Assessment: By comparing normal vs attack, we see how a few thousand malicious events (vs. hundreds of thousands of normal ones) can signal a severe security breach.

How We Use It

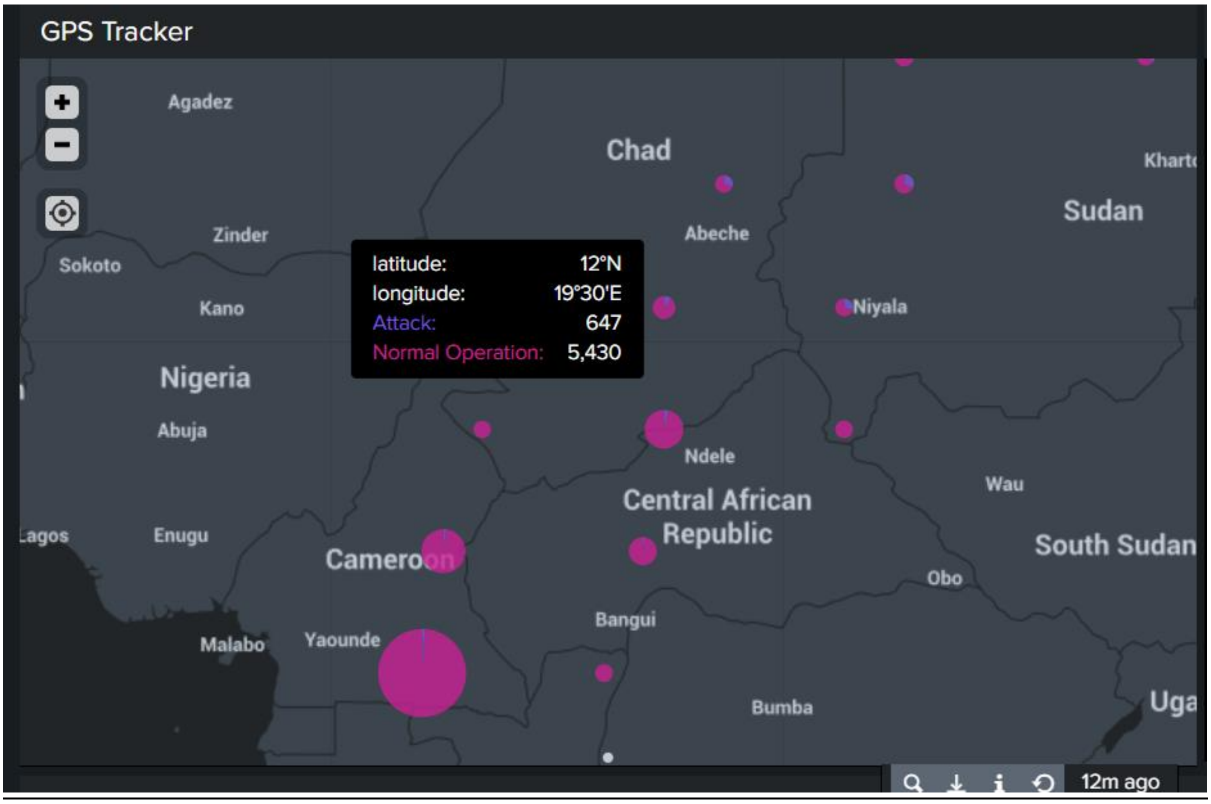
- Drill-Down: Click a spike to jump straight to raw logs for forensic analysis.

- Correlation: Combine with threat-intel alerts or NetFlow anomalies to confirm attack vectors.
- Reporting: Visual timelines make clear, evidence-backed reports to stakeholders.

In summary, the Attack Timelines panel gives us a concise, visual narrative of when and how our IoT devices were targeted-enabling quick detection, precise investigation, and effective response.

Device Behavior | Normal Operations Vs Attack

With the rise of smart homes, connected vehicles, and location-aware systems, understanding how these devices behave under normal and attack conditions is essential. I'll demonstrate how visual analytics may be used to identify anomalous trends, distinguish between malicious and neutral activities, and enhance threat identification in general of 5 IoT devices.



GPS Tracker

latitude: 12°N
longitude: 19°30'E
Attack: 647
Normal Operation: 5,430

Each pie chart represents a location where the device is operated, and its segments/ divisions shows the proportion of attack vs normal events. Size of each pie chart is showing the total number of events at that location which spots high-activity zones. Attack is in purple and normal operations are in pink color.

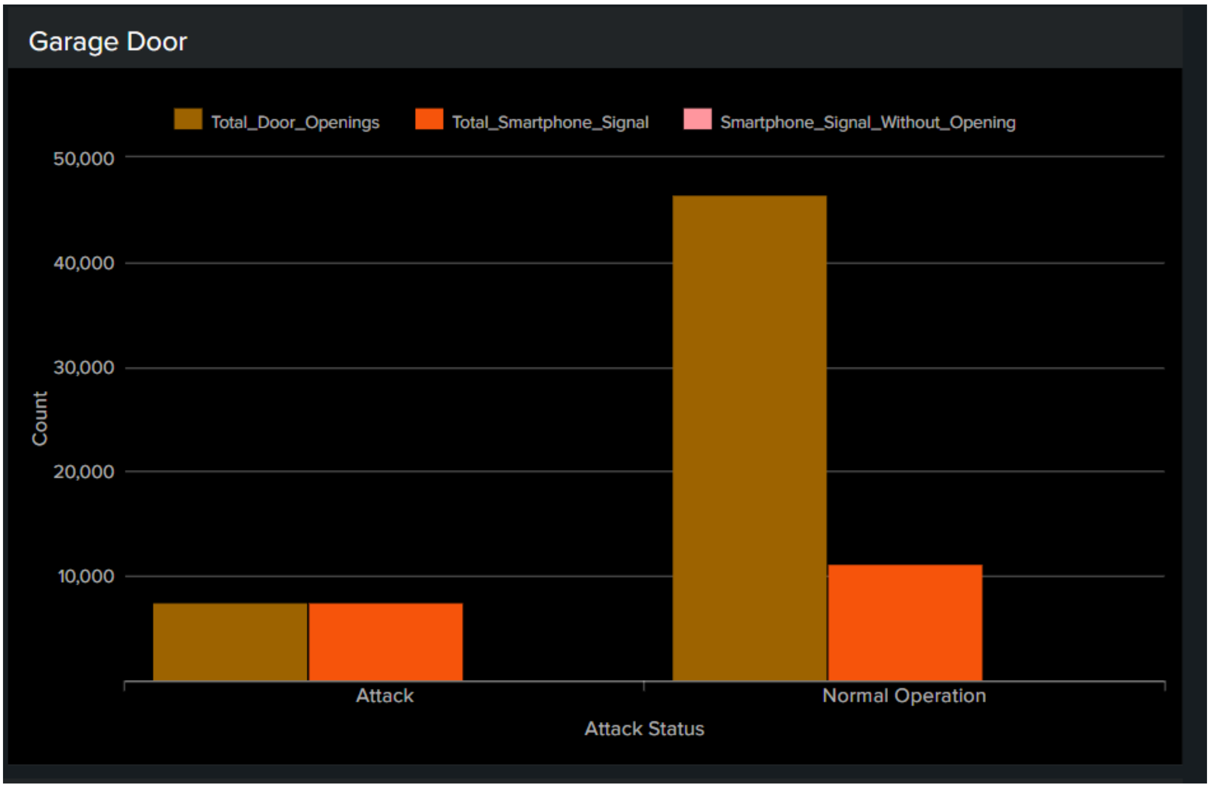
Why it's useful?

Can quickly spot where attacks are happening more frequently, which is useful to suggest solutions on targeted threat locations.

If the same device shows up in nearby locations with pattern, that might indicate GPS tampering.

How can be improved?

Heatmaps can be used to show attack density, different icons for each attack types, cross device correlation like compare gps behavior with other IoT devices.



This bar chart shows the counts of total door openings (door state= open/true), total smartphonesignal (true/signal came, false/not detected), smartphone signal without opening (signal-true, doorstatus=false)

As shown in fig, smartphone signals and door openings match in count, suggesting that during in attack situation every time a smartphone signal was detected, the door opened. A possible potential attack pattern where the garage door is being repeatedly opened several times.

In normal operations most door openings (approx. 35240) occurred without any smartphone signal, this could be if the user might be manually opening the door without their phone nearby.

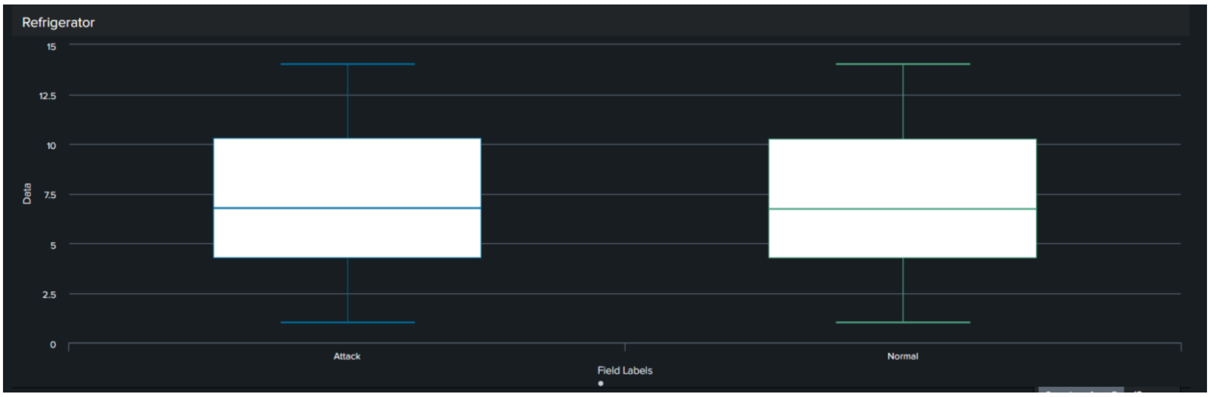
Don’t see any behaviors where smart phone signal detected and door didn’t open.

Why ?

Garage doors are critical entry points to a home, making them a prime target for IoT-based attacks, such as unauthorized access or remote control.

To find anomalous patterns, such as unexpected door openings without smartphone presence, are happening during attacks.

Fridge:



The box plot for Attack (blue) shows a median around 7, with the interquartile range (IQR) in the range of 5 to 10, The box plot for Normal (green) also has a median around 7, with a similar IQR based on fridge temperature.

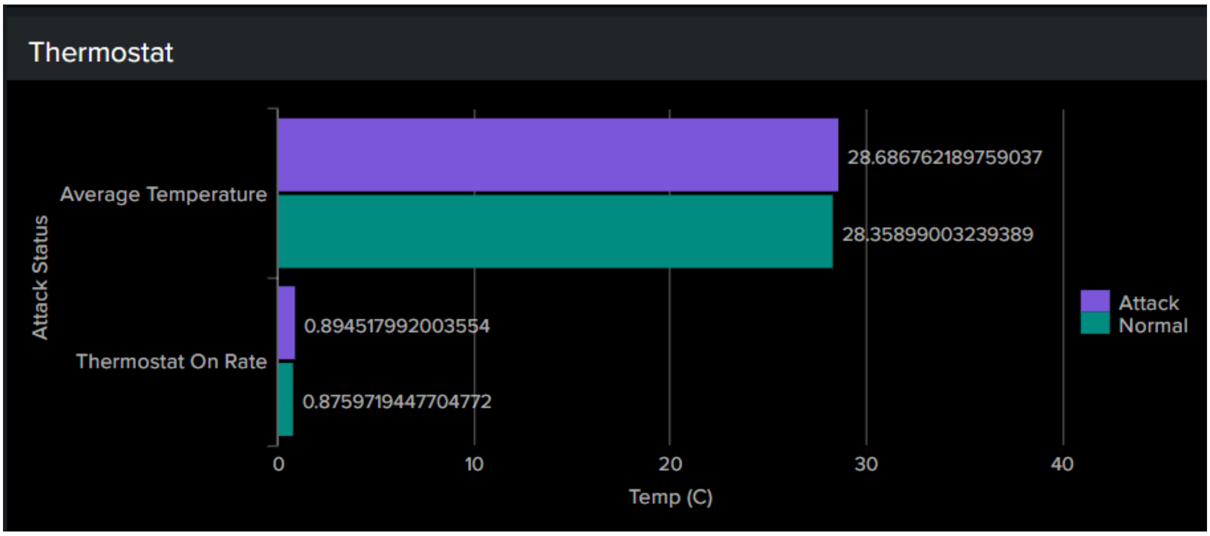
Here, the data metric for the fridge appears to be very similar under both ’Attack’ and ‘Normal’ conditions, this might need for deeper analysis to detect sophisticated attacks.

Why?

Refrigerators in IoT setups often monitor temperature, energy usage, or door status, and attacks could lead to spoilage, energy waste or data breaches, this could give us understanding how attacks might affect essential home appliances.

How can be improved?

Time series visualization of different metrics. Looking for sudden spikes, drops, unusual patterns, or deviations from the cyclical behavior of a refrigerator like cooling cycles.



This visualization is a horizontal bar chart showing the average values of two metrics in the x-axis for the 'Thermostat on rate(status on/off)' under ‘Attack’[purple color] and ‘Normal’ [blue] condition, and for Average Temperature.

During an attack, the average temperature is somewhat higher (28.69°C) than it is during regular operation (28.36°C). This slight increase might be a sign of an attack where the thermostat is being manipulated to overheat a room, which could lead to waste of energy or harm to the equipment that is sensitive to temperature.

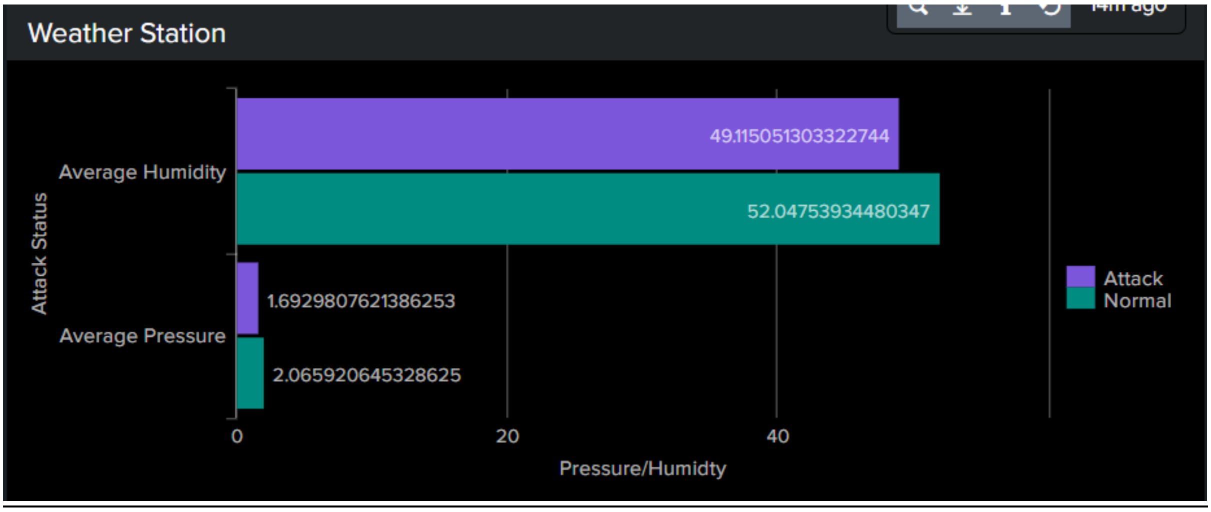
During an attack, the thermostat is on 89.46% of the time and on normal operation its 87.60%. This small increment raises the possibility that attacks may cause the thermostat to remain active longer (ON) or more frequently to maintain the higher temperature.

Why?

Thermostats are integral to smart home and building automation systems. They control heating and cooling systems, directly affecting a building's environment. A higher thermostat on rate during attacks can lead to increased energy consumption, raising costs.

How can be improved?

Statistical significance tests, correlation, how these metrics change over time for both normal and attack scenarios.



This visualization is a horizontal bar chart showing the average values of two metrics in the x-axis for the 'Thermostat on rate(status on/off)' under ‘Attack’[purple color] and ‘Normal’ [blue] condition, and for Average Temperature.

During an attack, the average temperature is somewhat higher (28.69°C) than it is during regular operation (28.36°C). This slight increase might be a sign of an attack where the thermostat is being manipulated to overheat a room, which could lead to waste of energy or harm to the equipment that is sensitive to temperature.

During an attack, the thermostat is on 89.46% of the time and on normal operation its 87.60%. This small increment raises the possibility that attacks may cause the thermostat to remain active longer (ON) or more frequently to maintain the higher temperature.

Why?

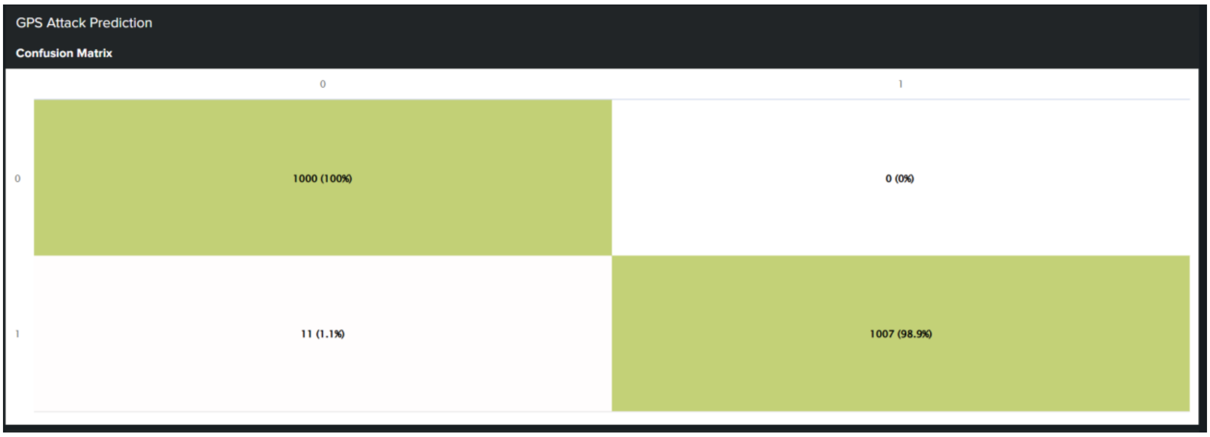
Thermostats are integral to smart home and building automation systems. They control heating and cooling systems, directly affecting a building's environment. A higher thermostat on rate during attacks can lead to increased energy consumption, raising costs.

How can be improved?

Statistical significance tests, correlation, how these metrics change over time for both normal and attack scenarios.

Attack Predictions using Machine Learning

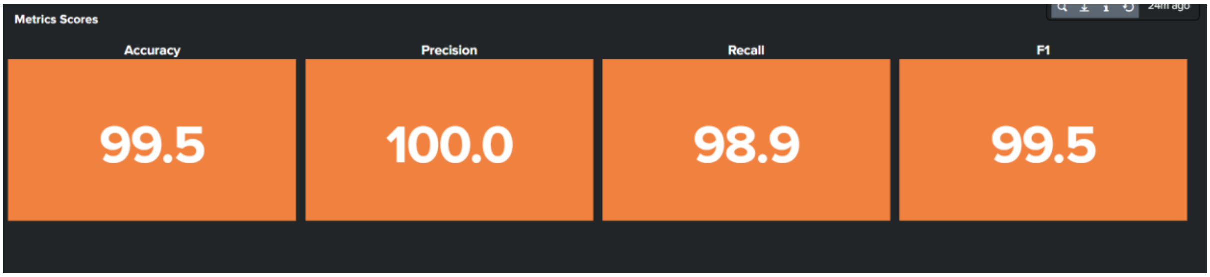
After noticing from GPS tracker figure , there seem to have some pattern where devices located nearby to regions having attacks. So, to analysis further we have used Machine learning toolkit in splunk to check few metrics with device data.



GPS Attack Prediction

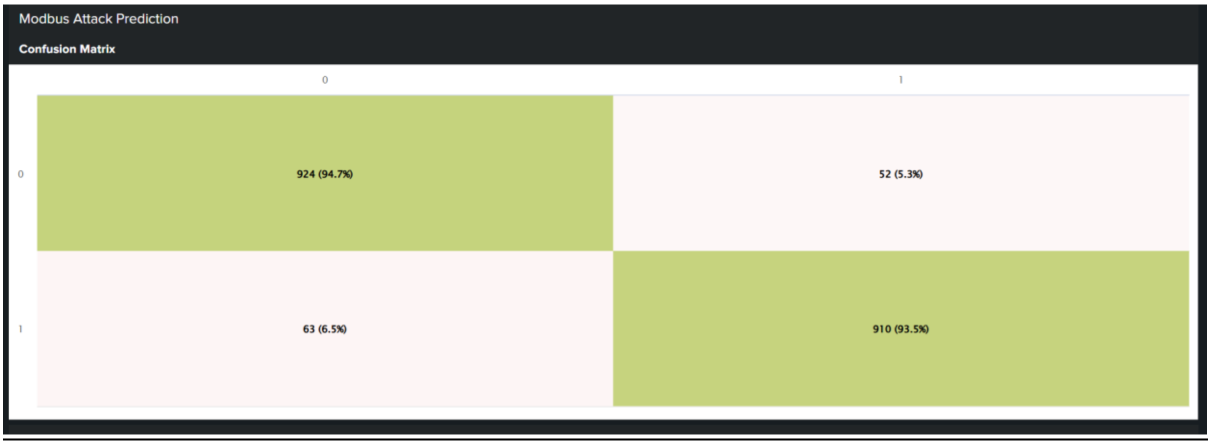
Confusion Matrix

	0	1
0	1000 (100%)	0 (0%)
1	11 (1.1%)	1007 (98.9%)



Metrics Scores

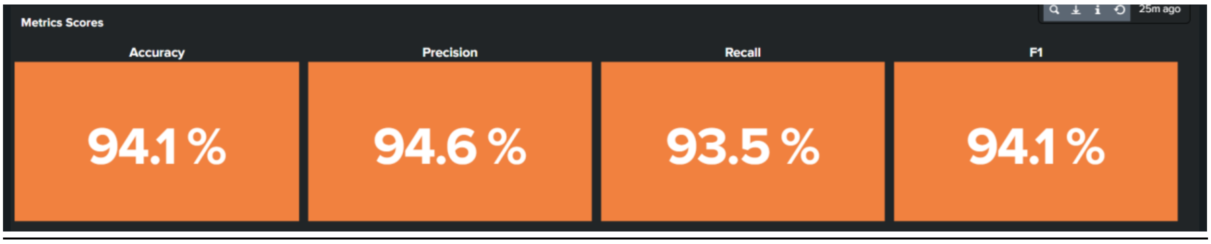
Accuracy	Precision	Recall	F1
99.5	100.0	98.9	99.5



Modbus Attack Prediction

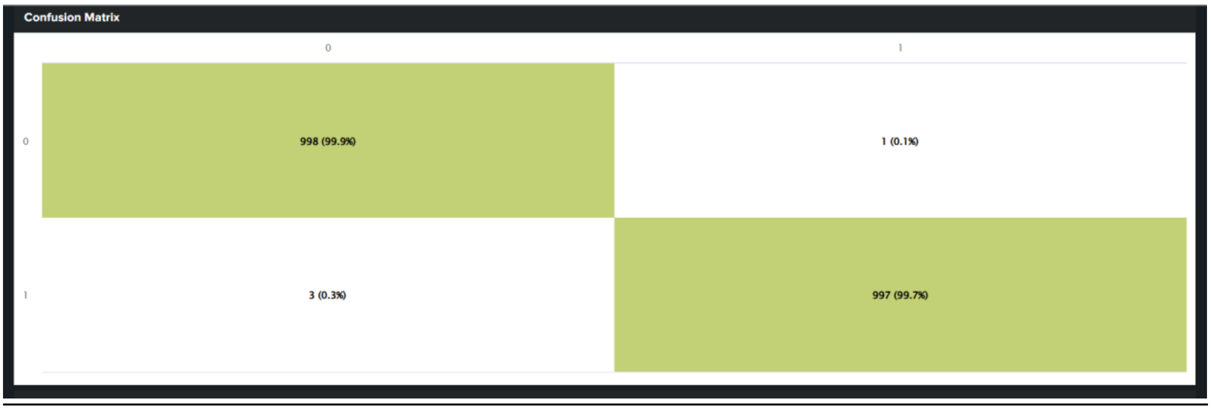
Confusion Matrix

	0	1
0	924 (94.7%)	52 (5.3%)
1	63 (6.5%)	910 (93.5%)



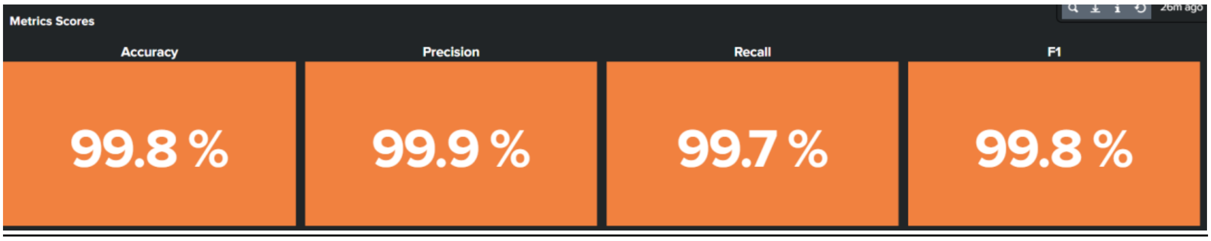
Metrics Scores

Accuracy	Precision	Recall	F1
94.1 %	94.6 %	93.5 %	94.1 %



Confusion Matrix

	0	1
0	998 (99.9%)	1 (0.1%)
1	3 (0.3%)	997 (99.7%)



Metrics Scores

Accuracy	Precision	Recall	F1
99.8 %	99.9 %	99.7 %	99.8 %