DataCraft Trio

Debnath Kundu (MT22026) , Pijush Bhuyan (MT22049), Snehal Buldeo (MT22074)

INDRAPRASTHA INSTITUTE *of*
INFORMATION TECHNOLOGY **DELHI**

Data Description

- Dataset URL - UCI Repository [detection_of_IoT_botnet_attacks_N_BaIoT]

- This public dataset contains real-time network traffic data recorded from nine commercial IOT devices that were infected with common botnet malware - **BASHLITE** and **MIRAI** to carry out ten types of network-based attacks.

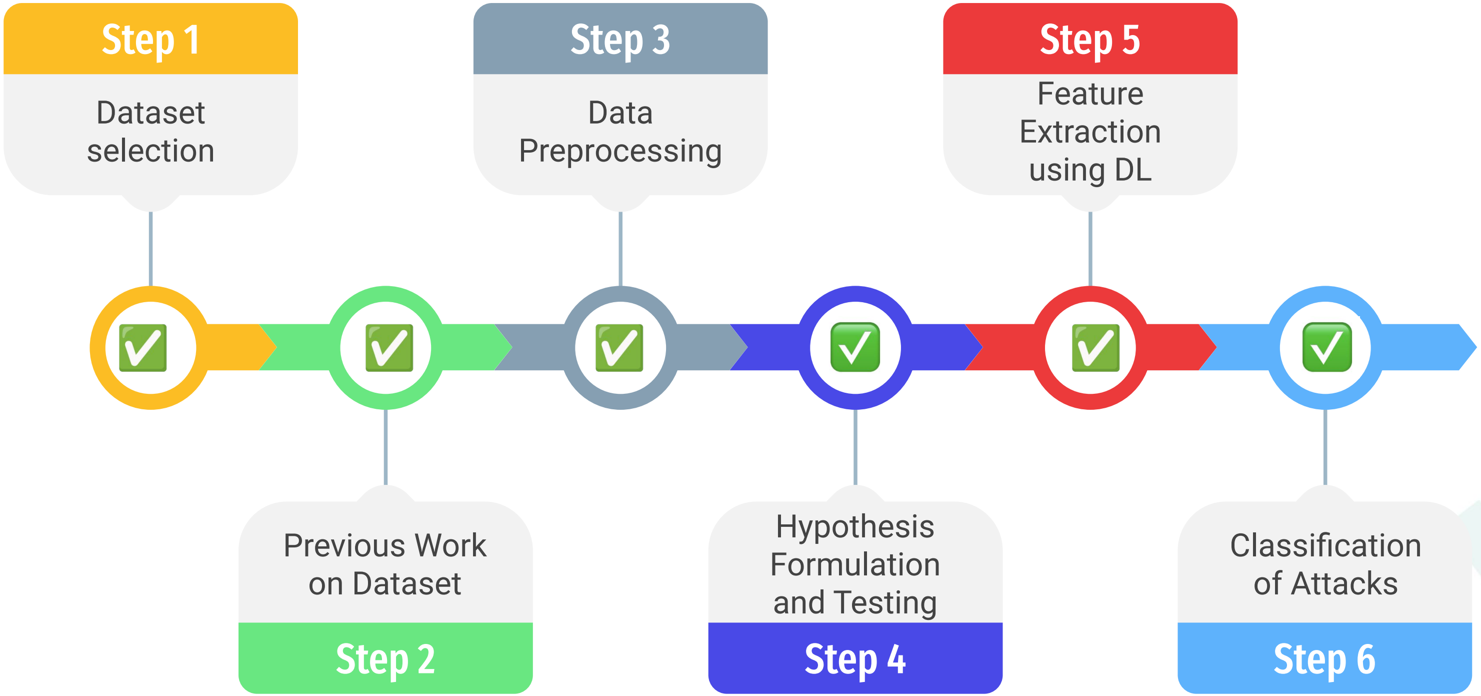
- **Types of IOT devices:** Thermostat, Baby Monitor, Webcam, Doorbells, and Security Cameras.

Types of Attacks

1. **BASHLITE MALWARE-MIRAI MALWARE -**
- **Scan:** Scanning the network for vulnerable devices
- **Junk:** Sending spam data packets
- **UDP:** Flooding the network with UDP packets
- **TCP:** Flooding the network with TCP packets
- **Combo:** Sending spam data and opening a connection to a specified IP address and

2. **MIRAI MALWARE -**
- **Scan:** Automatic scanning for vulnerable devices
- **Ack:** Flooding the network with Ack packets
- **Syn:** Flooding the network with Syn packets
- **UDP:** Flooding the network with UDP packets
- **UDP Plain:** UDP flooding with fewer options, optimized for higher PPS

Plan of Action and Progress So Far



Hypothesis Formulations

1. **Bashlite:**

   Scan attacks have similar packet flow across all devices

   i.e. $\mu_1 = \mu_2 = \ldots . \mu_9$ **[Don't Reject]**

2. **Mirai:**

   a. Scan attacks have similar packet flow for **Danmini Doorbell** and **Philips Baby Monitor** i.e. $\mu_1 = \mu_2$ **[Don't Reject]**

   b. Scan attacks have similar packet flow for both the **Provision camera models**

      i.e. $\mu_1 = \mu_2$ **[Don't Reject]**

   c. Scan attacks have similar packet flow across the **SimpleHome cameras** and **Ecobee thermostat** devices

      i.e. $\mu 1 = \mu 2 = \mu 3$ **[Don't Reject]**

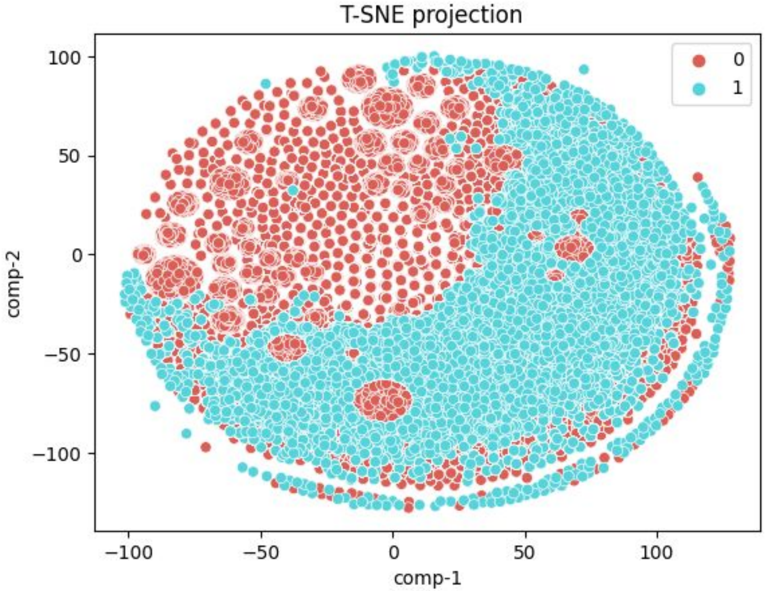
Further Tasks

1. **Unsupervised:** IOT Network Stream Anomaly Detection

2. **Supervised:** IOT Malware Attack Classification

Unsupervised Anomaly Detection in IOT Network Streams

- **Autoencoders** to learn & regenerate benign traffic with minimal error
- **AE** will not be able to regenerate malignant traffic with same error threshold. If **error > threshold**, flag as malignant.
- Benign and malignant traffic are well separated in the **AE** embedding feature space as shown in the **t-SNE** plot. [Rest also, separable]



Unsupervised Anomaly Detection in IOT Network Streams (Contd)

- **Accuracy** of AE trained on Danmini Doorbell for benign traffic and evaluated on mirai attacks. [Similarly, for others]

```
traffic type : Mirai-scan
Detected anomalies: 100.0%

traffic type : Mirai-ack
Detected anomalies: 100.0%

traffic type : Mirai-syn
Detected anomalies: 100.0%

traffic type : Mirai-udp
Detected anomalies: 100.0%

traffic type : Mirai-udp-plain
Detected anomalies: 100.0%
```

Classical ML Approach (**SVMs**)

- Device used : Danmini Doorbell
- Classes : **6** i.e. **1 Benign** + **5 types of mirai attacks**
- Explored linear, polynomial and **RBF** kernels
- Used AE for feature extraction and dimensionality reduction **(115 to 28 features)**

Kernel Type	**Linear**	**Polynomial**	**RBF**
Accuracy	0.51	0.43	0.56
Precision	0.51	0.49	0.47
Recall	0.52	0.44	0.57

Multi-Class Classification of Attacks

Classes

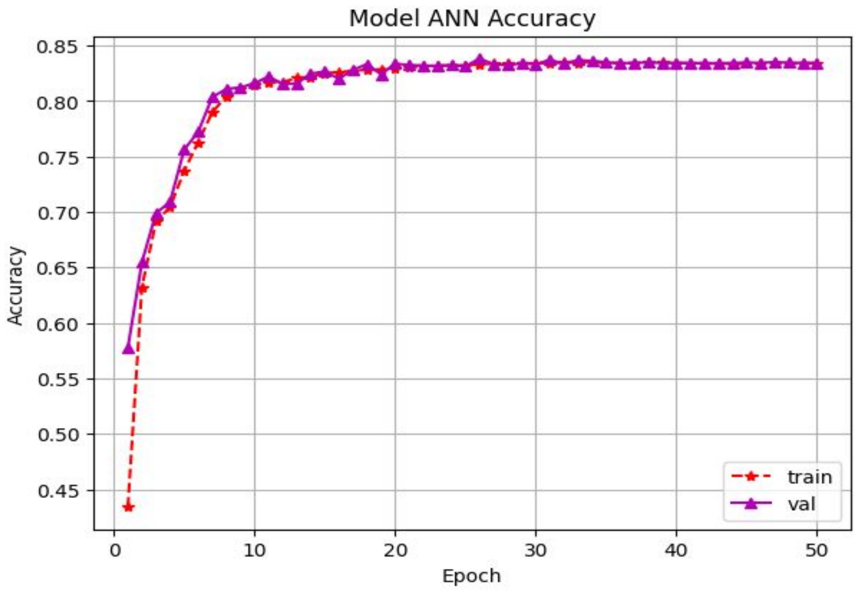
- **Benign ::** 1, **Bashlitte attack ::** 4, **Mirai Attack ::** 5

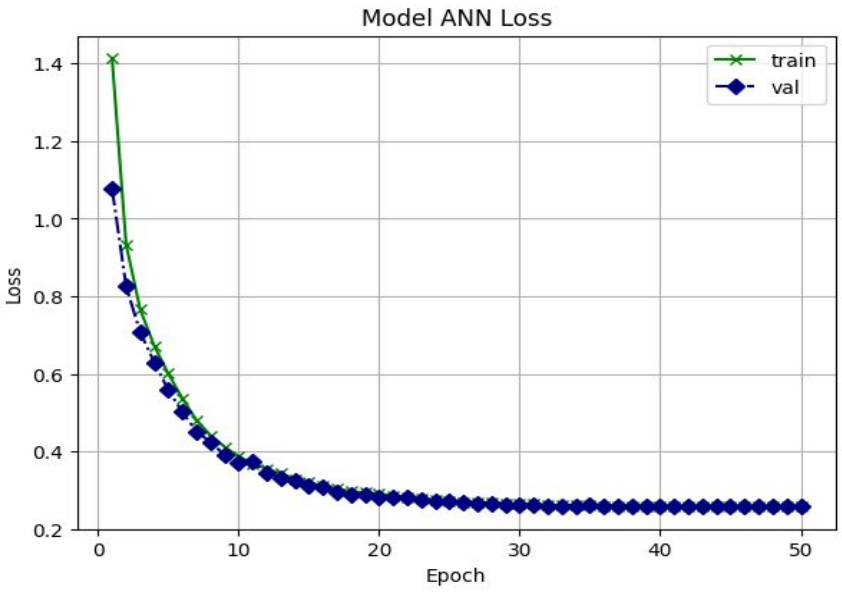
To study

1. Models trained to detect botnet attacks on various brands of **security cameras** are equally effective in detecting anomalies in **webcams**.

2. Models trained to detect botnet attacks on various brands of **security cameras** are not effective in detecting anomalies in other devices.

Training of Artificial Neural Network (ANN)



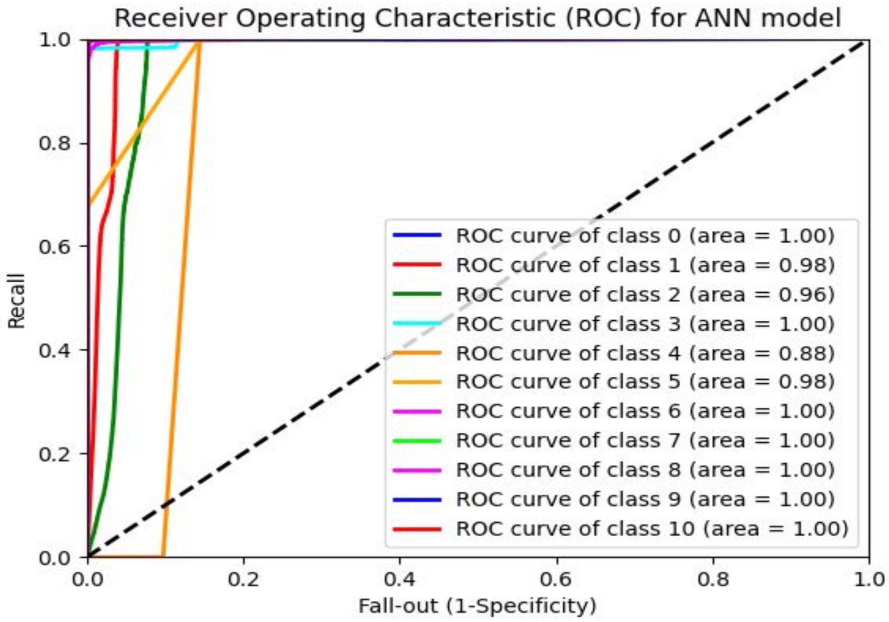


Device: **Provision_PT_737E_Security_Camera**

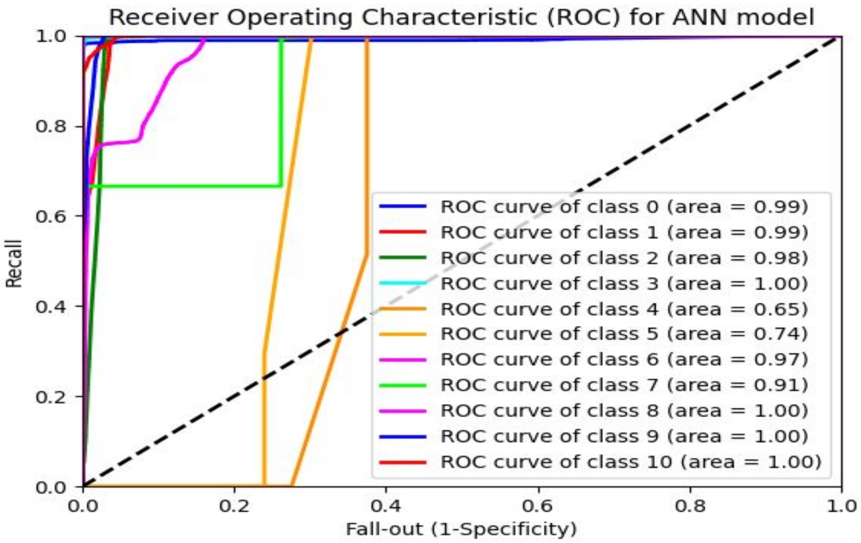
Test and Results on the same device

- Number of classes : 10
- 1 Benign and 9 malicious classes
- Device : **Provision_PT_737E_Security_Camera**

- Accuracy: **82.61 %**

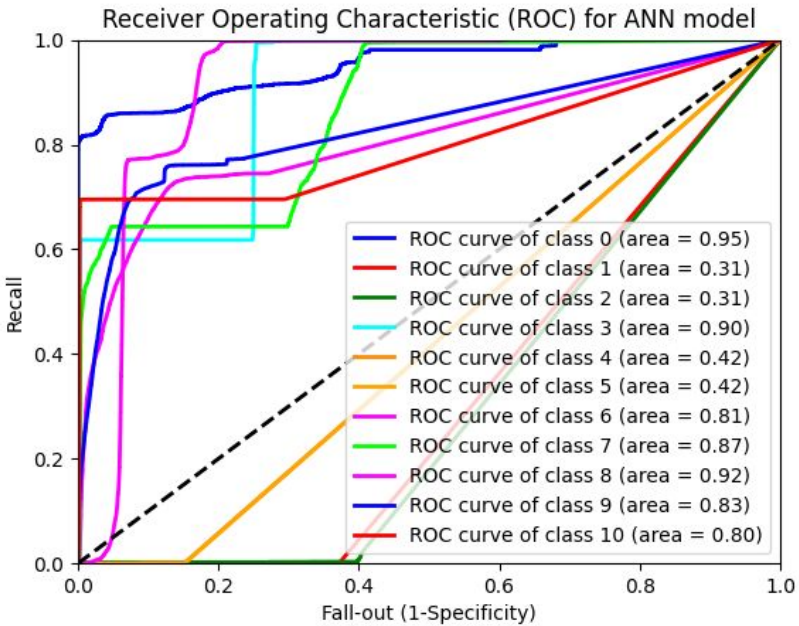


Test and Results on different device (same brand)



- Device: **Provision_PT_838_Security_Camera**
- Accuracy : 65.53 %

Test and Results on different device



Device: **Ecobee_Thermostat**

Accuracy : **44.39%**

Inference & Future Scope

- If we want to just detect an anomaly in the device, then unsupervised **AutoEncoder** based techniques perform well enough!

- However, if we need multi-class classification of each type of attack, then **ANNs** are more effective compared to classical ML models.

- **Future Scope** involves exploring sequential models (RNNs, LSTMs, etc.) for multi-class classification.

Thank You