**Proposed Attack Detection Framework**

**Motivation/Problem Statement**

The Internet of Things (IoT) is now widely used in various domains including smart buildings, power grids, entertainment, transportation, and health care. It is forecast to play a significant role in future technical revolutions, and its utilization is likely to increase exponentially over the coming years. Due to the increasing number of IoT devices and the massive amount of data associated with them, the issue of security in the IoT has been raised. Security in the IoT implies the need for the defence of IoT applications and the IoT infrastructure. Many IoT devices can be easily targeted by intrusion because they are connected with outside resources at the network layer, and they do not have proper security defence. As such, an attacker can compromise the network layer and obtain control over an IoT device, which can then be used maliciously, or it can compromise other nearby devices connected to it. According to a report from Statista, the number of devices connected through the Internet is expected to reach 75.44 billion. worldwide by 2025. The increasing number of IoT devices will provide many opportunities for attackers to compromise them through malicious emails, collusion attacks, and denial of service attacks among many other types of attack.

The existing mechanism for attack detection on wireless network works on the centralized cloud, which cannot satisfy the distinct requirements of the IoT, such as scalability, distribution, resource limitations, and low latency, to name but a few.

So, to ensure security of IOT devices and networks we have developed a fog- based attack detection mechanism to detect DDoS attack.

**DDOS Attack Detection Framework**

Alongside the development of Internet of Things (IoT), security attacks are also increasing day by day. So our model is basically proposed to detect attacks in IoT, wherein an attack detection system is deployed at the central point in the network that collects data from the network and classifies it as “attack” or “normal” using a supervised machine learning algorithm.