GITAM School of Technology
Department of Computer Science and Engineering
Bengaluru

Botnet attack in IoT

Speaker: Ms. Geetha K, Research Scholar, CSE, GST, BLR		
Date: 03/06/2024	Time: 11:00 AM	Venue: SB 535

Title: "Securing the Internet of Things against Botnet Attacks using Deep Learning Techniques"

Research Background

The Internet of Things (IoT) is a network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, and connectivity which enables these objects to connect and exchange data. The IoT allows for the seamless collection and analysis of data in real-time, enabling various applications and services to be developed based on the insights gained from the data. The Internet of Things (IoT) has a wide range of applications in various industries and domains.

The IoT is vulnerable to various security challenges due to its widespread use of interconnected devices and systems. A botnet attack in the Internet of Things (IoT) involves the compromise of multiple connected devices, such as smart home appliances or internet-connected cameras, and the use of these devices to perform malicious activities. In a botnet attack, an attacker can take control of the compromised devices and use them to launch coordinated attacks, such as Distributed Denial of Service (DDoS) attacks. The effects of a botnet attack in IoT can be far-reaching and potentially damaging, both to the individual devices involved and to the wider network.

Machine learning and deep learning techniques can be used to detect botnet attacks in the Internet of Things (IoT) by analysing network traffic and device behaviour. Machine learning algorithms can be trained on large datasets of network traffic to identify patterns and anomalies that are indicative of botnet behaviour. Deep learning algorithms can also be used to identify botnet activity, especially when dealing with large amounts of complex data, by modelling the underlying relationships and dependencies in the data.