# Related works

1) Several research papers are available on IoT devices and security issues faced by IoT devices. Most of the research are focusing on or are related to the problem statement that is at hand. In this paper [1], the Authors focuses on DDos attacks for IoT devices using Aircrack-ng carried out to reject fundamental services to microcontroller (NodeMCU) which is a gateway device. The system prevents most forms of attacks that target the victim IoT device using their MAC addresses. System has DHT11 and NodeMCu sensor. The system avoids most types of attacks using their MAC addresses targeting the victim's IoT devices. For this, it should serve as a station in order to connect to an access point. Therefore, proposed solution is that it adds an additional layer of security to the gateway by constantly changing its MAC address. Since MAC address is specific it’s easy for an attacker to launch an attack to the gateway by specifying the MAC address of the gateway device. By this proposed solution, we can change the MAC address continuously so that it becomes hard to find the its address of the gateway thus adding another layer of the security to gateway.

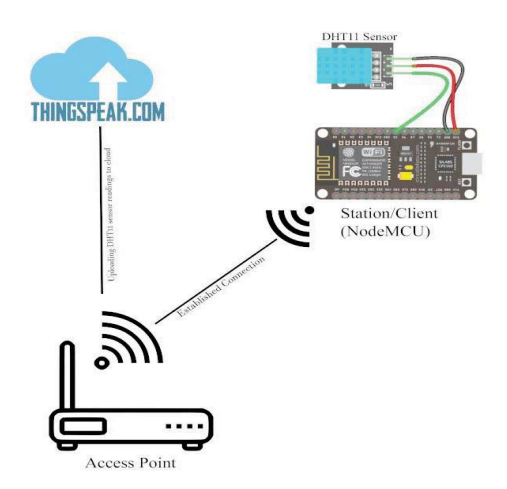


Figure 1 System Architecture

2) In this study [2], the authors demonstrate the Ddos attack Detection-IoT system using machine learning method. They use pandemic modelling sources for IoT networks consisting of WSNs. In order to detect and abnormal defense behaviours, they establish a proposed framework. There are major difficulties, given the effect of IoT-specific features such as inadequate computing capacity, power constraints, and node density on the creation of a botnet. They use standard datasets for Mirai attacks which is the famous attack. They also use many machine learning methods. Data is collected and extracted from several IoT devices. There were many challenges for authors. These are dataset preparation, data preprocessing. The proposed framework reveals any strange movement by searching the traffic for IoT devices. In the experimental results, they found that the combination of random forest and decision tree algorithm achieves high accuracy for detection.

3) In this research [3], the authors simulate IoT network with 100 nodes using the simulation tool OMNET++ which includes DDos attacks and is based in three tier IoT architecture. Also, OMNET++ simulator is a C++ based component simulation library. It provides a platform for the models to be generated. This 3-Tier architecture is composed of Perception Layer, Network Layer, Application Layer. In order to calculate the accuracy of detecting DDos attacks on IoT networks using machine learning techniques, regular and attack-injected traffic is generated. A new IoT dataset is created by authors with different scenarios of normal traffic and traffic with attacks of different intensities. Due to the lack of public datasets, the main contribution of this research is the recognition of the need for an IoT DDos attack dataset. Therefore, this created dataset used with machine learning tools to determine accuracy of the DDos detection. Different ML algorithms in Azure ML studio used to analyze created dataset and evaluate the accuracy of the detection. The algorithms in research such as decision forest, decision jungle and boosted decision tree were used. Performance comparison of boosted tree in detecting DDos attacks is higher than other two algorithms. The authors made this dataset publicly available. The dataset can be applied to different machine learning algorithms in order to develop different defensive mechanism to DDos attacks.

4) In this article [4], the authors present the framework for detection of the depletion type DDos attacks using Matching Pursuit algorithm. They use multiple network traffic features simultaneously to effectively detect low density DDos attacks. The proposed method uses a dictionary created from network traffic parameters using KSVD algorithm. Network traffic dictionary generation offers legal traffic models and attacks. They discussed Wavelet and MP based DDoS detection approaches. These are, MPMP, Adaptive Matching Pursuit Based Detection (AMP), and Wavelet-based intrusion detection methods. In the AMP method, they combined anomaly detection and misuse detection using decision engine. And also,

They evaluated both methods with and without the decision engine for the detection of TCP and UDP flood attacks. They also combined TCP and UDP flood datasets to test the efficiency of the methods in three traffic groups to detect DDos attacks. Authors evaluated and compared these approaches using CAIDA datasets which are used as a combination of two datasets containing only DDoS attacks and only attack free traffic. And also, these approaches is compared and evaluated using BOUN DDos dataset. As a result of this, They also implement DDos detection methods using Matching Pursuit and Wavelet techniques and compare them using two distinct dataset. The experimental results show that the AMP method performs better compared to the Wavelet and MPMP methods with higher CID values.

References