**INTRODUCTION**

Today, we are living in the society where many things are going to be automated and digitalize. Technology is now involving in our daily life and there are many simple examples for that such as mobile phones, personal computers etc. Converting things to smart devices and making these processes automated, IoT is one of the technology which plays an important role for that purpose. So we can say that it is one of the most important technologies for businesses as well as for our daily life. But, it is important to remember that as the technology increases there are also a number of issues increases related with that technology. Similarly, as the number of devices connected it means the more information is sharing between these devices and if there is any type of bug in the sharing system, there is a chance that each connected device could corrupt and confidential information could steal by the hacker.

There should be an international standard for compatibility of IoT here which is not yet, therefore it is very difficult for devices which are manufactured from different companies to communicate with each other. Also there are many IoT devices which requires and ask to input user personal information such as name, location and contact as well as data which are important to hackers such as social media information. Therefore, the information sharing between IoT devices needs to be secured. Also IoT privacy and security are cited as major concerns. There are number of attacks on IoT including malware. Malware can be defined as a malicious software or bug which is designed to gain access and damage your device, device could be computer or IoT device.

IoT devices are vulnerable to network attacks therefore, malware and network attack detection in IoT is the focus of research in recent years. There are many workings are there to address the issue and detect network attacks. In comparison, ML and DL which can be defined as machine learning and deep learning in artificial intelligence has the power to detect unknown network behavior by automatically learning the networks attacks and malware patterns based of large datasets. In this paper we will focus on the security aspect of networks of IoT by understanding the use of machine learning based algorithms in artificial intelligence for the detection of network attacks and malwares. For this purpose, we will consider Aposemat IoT-23 which is a labeled dataset and created in the Avast laboratory. This dataset also provides benign IoT traffic which is helpful to develop or implement machine learning based algorithms in artificial intelligence.