**1    INTRODUCTION**

1.1.    Background and Basics

The internet of things, or IoT, is a system of interrelated "things " that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.  These "things" could be computing devices, mechanical and digital machines such as build in sensors, monitors etc.

A good example of a network of IoT devices is the security system implemented by various locations which include, CCTV cameras, motion sensors, automatic locks, smoke detectors, temperature sensors etc.

IOT devices are becoming pervasive. They are used extensively in a lot of fields and their utility is just going to keep increasing. IOT devices help to automate things, reduce labour costs and facilitate smart living.

Hence, it is important to build an optimal system that can provide proper safety and security measures for IOT devices.

An intrusion detection system is one such system that can be a building block in making the IOT network as secure as possible. An intrusion detection system is a system that passively monitors the data exchange in the network and of the network with externals entities and looks for malicious activities that can be classified as an intrusion or attack. It then notifies the user or sends a notification to some other system which may or may not take action against the detected intruder. Simply put, if the network of devices is a home, an intrusion detection system is a CCTV camera.

Also, a step up from just a intrusion detection system is an anomaly based intrusion detection system. This type of system creates a profile of normal behaviour, and any activity that falls outside of the normal category is marked as anomalous. Anomaly based system is better suited to defend the system against zero-day attacks.

There are certain challenges while building this system which are specific to IOT devices. For example, the low computational powers and limited amount of resources (such as space/memory). The IDS system should be build keeping in mind all these challenges and they should be overcome in the most efficient manner.

2   PROJECT PLANNING AND MANAGEMENT

2.1.    Project Process Model

Iterative waterfall model is the best suited for this project.

Iterative waterfall model can be thought of as incorporating the necessary changes to the classical waterfall model to make it usable in practical software development projects. It is almost same as the classical waterfall model except some changes are made to increase the efficiency of the software development.

The iterative waterfall model provides feedback paths from every phase to its preceding phases, which is the main difference from the classical waterfall model.

In our project, every phase is well defined and to be executed one after the other sequentially, like the waterfall model. But if need be, there is space for going back to previous stages making changes.

Hence, iterative waterfall is to be used for this project.