**Vulnerabilities and Exploits in IOT Communication**

**(Top of The Application Layer)**

Mohamed Razmeen

*MSc Information Technology (Specializing in Cyber Security)*

*(Std No: MS21908910)*

**Introduction**

Nowadays IOT devices are everywhere in future every device will be interconnected with IOT. for an example smart houses, smart cities, smart industrial operations etc. Meanwhile there are so many vulnerabilities and exploitations in IOT security. Currently there are so many security solutions are given by cyber security experts and IT experts who are related to IOT security but still there are some vulnerabilities exist in M2M communications and unsecured communications between devices. This research based on vulnerabilities and how to handle and minimal them.

**Problem Statement**

IOT devices are everywhere and essential for every sectors. There are so many micro controllers to perform IOT based projects and applications, however the problem is how they are communicating each other and is the communications are secured. For an example we can use a Node MCU as microcontroller and we have to handle the request response made by client side and the server side, if the parameters and path variables are not encrypted or secured intruders can easily exploit the vulnerabilities.

**Methodology**

Communication protocols are major part in IOT platforms. I supposed to research about the communication protocols and standards that are commonly used in IOT development and refer the research and review papers that are related to my research Topic.

**End Goal**

There are different types of protocols used in IOT platform, this research will be focused on how to secure request and responses parameters, path variables top of the application layer and try to make a demonstration or implementation regarding the topic.