NIELIT, Gorakhpur

Course Name: A-level (1st Sem.) **Subject: IoT**

Topic: IoT security **Date: 18.05.2020**

As the name suggest IoT i.e Internet of Things means every physical device is connected to each other by Internet this creates opportunities for attackers. Vulnerabilities of attack is broad, even for a single small device. The risks posed include device control, data transfer, data manipulation, device access, malfunctioning devices, and always-on/always-connected devices.

The main challenges in security remain the security limitations associated with producing lowcost devices, and the growing number of devices which creates more opportunities for attacks.

Challenges

- **Unpredictable Behavior** – Devices available connected through internet and it need to be updated by user often result in devices running on outdated software, leaving them open to newly discovered security vulnerabilities.
- **Device Similarity** − IoT devices are fairly uniform. They utilize the same connection technology and components. If one system or device suffers from a vulnerability, many more have the same issue.
- **Problematic Deployment** − IoT devices are always placed on advanced networks and analytics where they previously could not go. Unfortunately, this creates the problem of physically securing the devices in these strange or easily accessed places.
- **Long Device Life and Expired Support** –the benefits of IoT devices is longevity, however, that long life also means they may outlive their device support. Compare this to traditional systems which typically have support and upgrades long after many have stopped using them because of some new technology came in the market. Orphaned devices and abandonware lack the same security hardening of other systems due to the evolution of technology over time.
- **No Upgrade Support** − Many IoT devices, like many mobile and small devices, are not designed to allow upgrades or any modifications. Others offer inconvenient upgrades, which many owners ignore, or fail to notice.
- **Poor or No Transparency** − Many IoT devices fail to provide transparency with regard to their functionality. Users cannot observe or access their processes, and are left to assume how devices behave. They have no control over unwanted functions or data collection; furthermore, when a manufacturer updates the device, it may bring more unwanted functions.
- **No Alerts** − Another goal of IoT remains to provide its incredible functionality without being obtrusive. This introduces the problem of user awareness. Users do not monitor the devices or know when something goes wrong. Security breaches can persist over long periods without detection.