**Course Name: -** **Internet of Things (IOT) Security concepts**

**Course Details/Synopsis –**

One of the most dynamic and exciting developments in information and communications technology is the advent of the Internet of Things (IoT). Although networking technologies have become increasingly ubiquitous over the past two decades, until recently they have largely been restricted to connecting traditional end-user devices, such as mainframes, desktop and laptop computers, and, more recently, smartphones and tablets.

Recent years have witnessed the attachment of a much broader range of devices to the network. These have included vehicles, household appliances, medical devices, electric meters and controls, street lights, traffic controls, smart TVs and digital assistants such as Amazon Alexa and Google Home etc. Industry analysts estimate that there are currently more than eight billion such devices connected to the network and project that this number will expand to more than 25 billion by 2020. The increasing deployment of these devices has enabled new use cases for network technologies. Some experts project that the IoT may generate as much as US$13 trillion in revenue by 2025.

Everyone who has used the internet is well aware of the onslaught of cyber-attacks that bombard computers nearly every day. Viruses, worms, trojans, botnets and other forms of malware have become all-too-familiar parts of the online experience, as are persistent efforts to hack through security.

The security of IoT devices has been a cause for concern for some time and has had the inevitable consequence of allowing both small- and large-scale attacks. Most of these attacks originate from simple security problems, for example, the retention of default passwords on a telnet service.

Purpose of this course is to expose the trainees to new developments in the areas of cybersecurity for the Internet of Things (IoT).

The course will cover the following

1. Introduction to IOT.
2. Fundamentals to Cyber Security.
3. Security in IOT covering cyber-physical systems, vulnerabilities, attacks, and countermeasures.
4. Security architecture and engineering for development of IOT system.
5. Standards and best practices in IOT Security.
6. Security in IOT lifecycle.
7. GRC for IOT, legal and regulatory requirement including auditing framework.
8. Interaction with industry regarding IoT deployments.
9. Case Study: Implementation of IOT Security in Biometric Registered devices.

**Justification/Rationale: -**

Recently, Internet of things (IoTs) has become the main issue in designing monitoring systems such as smart environments, smart cars, and smart wearable devices. IoTs has transformed the life of people to be more adaptable and intelligent. For example, in a healthcare monitoring system, using smart devices will improve the performance of doctors, nurses, patients, and the healthcare industry. The IoTs revolution is known as the fourth industrial revolution and would change the way humans interact with machines and lead the way to a high-technology machine-to-machine interaction. In fact, almost every device around us would be connected to Internet, collecting and exchanging data with other devices on the cloud.

Most of the countries around the world are adopting and deploying IOT devices in various sectors for automation and improvement of services and with increase of deployment of IOT, cybersecurity risk is also increasing parallelly. Hence learning of various cybersecurity threats & risk and mitigation of threats & risk in IOT technology is very important for policy makers, regulators, licensors, service providesof partner developing countries. This is why NTIPRIT has proposed a course on “Internet of Things (IOT) Security concepts” for ITEC Partner Developing Countries. As IOT is new and also it is coming along with 5G technology which will have use cases in all sectors including Agriculture, Health, Transport, Industry etc, the capacity building in the field of IOT security concepts for the stakeholders is very important.

**Aim and objectives of the course –** The course aims to impart knowledge about Internet of Things (IOT) Security concepts to the various stockholders like telecom policy maker, telecom regulators, IT service providers of various sectors including Healthcare, Agriculture, Transport, Industry etc.

The objective of the course for the participants are the following: -

1. Familiarize the participants with the basic concepts of Internet of Things (IOT).
2. Familiarize the participants with the fundamentals of Cyber Security.
3. Explaining the various vulnerabilities, attacks, and countermeasures in the IOT devices and IOT network.
4. Explaining the security architecture and engineering for development of IOT system.
5. Familiarizing the participant with Standards and best practices in IOT Security.
6. Explaining the IOT Security lifecycle and Digital Supply chain.
7. Explaining IOT legal & regulatory requirements.
8. Explaining the architecture of Biometric Registered Devices.