**8 Types of Security Threats to the IoT**

**Introduction**

The IoT industry is currently booming at a rapid scale, allowing for insights backed by data to provide value to industries and enterprises. For instance, in supply chain, IoT is helping track the exact locations and condition of the cargo shipments to ensure that goods in transportation safely reach their destination. In agricultural sector, IoT devices help farmers to monitor changes in weather near crop fields to enhance labor, harvest health and water usage. Travel industry is making use of IoT sensors to notify on-arrival passengers when their luggage reaches the airport.

These and many more opportunities offered by IoT are making our lives easier and provide us with limitless services to enable increased work productivity and efficiency. However, its adoption is still not as widespread as anticipated. The reason is the security obstacles associated with IoT devices. In the year 2018, according to a survey by Bain & Company, security was the top reason for industrial and enterprise respondents to not adopt IoT technology. These security challenges can be overcome, but to understand how to do that, it’s important to first know what these challenges are.

Let us look at some of the many security threats faced by the Internet of Things.

1. **Radio Frequency (RF) Jamming**

Hackers can use radio jamming to block wireless IoT devices by interfering with wireless communications to hinder their functionality. This can be done by getting hold of an RF Jammer, causing IoT devices to limit their communication ability by losing connectivity. For instance, residential and commercial wireless security alarms that are connected over a cellular network can be easily jammed and enable an intruder to break in without the knowledge of the security provider.

1. **Distributed Denial of Service (DDoS) Attacks**

A DDoS attack happens when all network devices are precariously made to send limitless messages that eventually cause congestion in the IoT network shut it down. Cyber criminals use DDoS attacks to control numerous compromised devices, thus preventing important information from reaching its destination.

1. **Privacy Leakage**

An unsecured IoT device that leaks its IP address, if identified by a hacker, can be misused to point to any location. It is recommended that IoT connections should be secured using Virtual Private Networks (VPNs). Just as an Internet Service Provider’s network can be secured by installing VPN on a router to encrypt all traffic passing through (see [HughesNet Internet](https://satelliteforinternet.com/hughesnet-gen5-internet-plans/) for the best satellite internet services), the same can be applied to an IoT device to ensure that your IP is private and your smart network is protected.

1. **Network Hacks**

A network hack takes place when an IoT device is compromised through the network that it is connected to. This kind of security breach allows a hacker to access and control the device. For instance, they can gain control of the thermostat of an industrial furnace and start a fire or cause an autonomous vehicle to crash by controlling its driving.

1. **Home Intrusion**

This is one of the reasons why smart homes are not ideally seen as a reality and adapted far and wide till now. It is also one of the scariest scenarios which can turn a device meant for an individual customer’s convenience into a major threat to their home privacy. Unsecured IoT devices that are shipped to a user with default username as ‘admin’ and password as ‘12345’ are very vulnerable to home intrusion. This can not only be used in planned burglaries but also invades complete privacy of a residential household. This is why it’s very important to secure a device’s credentials and connect them through a VPN.

1. **Lack of Device Updates**

Companies are manufacturing IoT devices at an increasing rate due to the growing demand. However, since their focus is on production and competition, manufacturers are not very careful with handling IoT device-related risks and security issues. Many of the devices in the market do not have considerable security updates, and some of them are never updated at all. Even if a device initially caters to security requirements, it becomes insecure and vulnerable after the emergence of new technologies and new cyber security challenges, making it more prone to cyber-attacks, especially if it is not updated.

Some manufacturers deliver Over the Air (OTA) firmware updates but stop doing that once they start working on next generation devices, thus leaving the older devices exposed to security threats.

1. **Unsafe Communication**

Most of the IoT devices do not encrypt messages while communicating over a network, which makes it one of the biggest security challenges of IoT. To prevent from intrusion, companies need to secure and encrypt their communication between cloud services and devices. Using transport encryption and standards such as TLS can ensure safe communication. Also, device isolation using different networks can ensure a secure private communication.

1. **Difficulty in Determining a Device’s Compromised Status**

Another one of the challenges of an IoT device is that it is very hard to ascertain if a device is hacked or not. Especially when there are a large number of IoT devices, it gets very difficult to monitor the security status of all the devices. This is because IoT devices need services, apps and protocols to communicate; and with more devices, it’s becoming unmanageable to find out which of them are compromised. As a result, many such hacked devices continue to work without the user’s knowledge and their data and privacy keeps getting compromised.

**The Bottom Line**

There is no doubt that IoT promises a change that can bring more convenience to our lives and is destined to get bigger with time. However, the bigger it is going to get, the more headaches it will progressively carry along with itself as the accompanying IoT trends and threats also get bigger. This can only be overcome if device manufacturers and IoT industry stakeholders take security seriously and make it a top priority instead of joining a competitive race towards more production and short-term profits.