# Top 5 IoT Security Challenges

When we talk about the era of digital transformation, we instantly think about IoT. It would not be wrong if we say that IoT is the next-generation interconnection paradigm. It allows connectivity amongst machines and devices without the need for human interaction. IoT is the high-end technology behind self-driving cars and the most innovative cities. A basic IoT application has the potential to make huge differences by collecting data and insights for companies.

With every passing day, more businesses are embracing IoT technologies. However, this brings with it a number of new challenges and difficulties. The IoT network is complex because of the large number of devices on the internet. Thus, there is a huge amount of data on the internet, which is constantly increasing. It is easy for hackers to attack IoT because the devices in the IoT ecosystem are easy targets. Let's take a look at some of the risks involved in IoT.

### ****Outdated IoT Devices and Unsatisfactory Software Testing****

The number of IoT-connected devices has almost reached 23 billion all around the globe. By 2020, this figure increased to 30 billion, and by 2025, it is likely to reach 60 billion. See how fast it is growing!

IoT is making its way into highly developed connectivity, automation, and customization. But there are dozens of challenges and issues regarding IoT business development gadgets. The first and foremost issue is that IoT devices do not receive enough security updates.

Usually, businesses provide firmware updates for just a short time period. They overshadow the vulnerabilities and challenges followed after the release of a new device. It is taken as a betrayal by the users who trust the company but are put forward to potential threats and attacks. Outdated hardware and software is of significant danger to the users.

### ****Increasing Use of Cryptocurrency Appeals to Hackers****

Cryptocurrency has been all over the news recently, and its growth is no secret. The growth of this virtual currency is undoubtedly attractive for traders and investors, but hackers have also got an eye on it. As useful as it is for [online payments](http://www.cardzgroup.com/ScratchCard.html) and money transfers, the high profit generated digital currency is also prone to cyber hackers, and we cannot ignore this fact. The number of attacks is gradually increasing, and essentially, it is not necessarily on the blockchain only. Thus, we cannot just say that blockchain technology is at risk; the whole application development process is at stake.

Numerous blockchain companies are improving their security and control hacking to provide a more secure environment to their users. Still, the number of attacks on the blockchain technology is continuing to rise.

### ****Ransomware and Malware Influencing IoT****

Back in 2018, the Sonic Wall reports unraveled some astonishing facts. The reports estimated that the IoT malware and encrypted threats had increased from 215.7 percent to 32.7 million. With the increase in IoT devices, the number of malware infections is also growing. The ransomware attacks are so strong that they can cripple the functionality of the device, and steal all the personal information and data of the customers.

### ****The Problem with Default Password****

The Mirai botnet or bad malware causes the gigantic and disruptive malware attacks. The most common reason for its success is weak login credentials and details. It leaves most of the IoT devices at immense risk specifically because of brute-force attacks and password hacking. The shipping procedure is a particular target of the Mirari botnet. Usually, shipping procedures have default login credentials, and they do not highlight it to the user to change it. Thus, the users are vulnerable to cyber-attacks.

If your IoT devices have weak passwords for login, you are more prone to hacking. Thus, considering this issue, governments prefer manufacturing trade against the selling of IoT devices that have default credentials. Usually, the default password and login are something like 'admin.'

### ****IoT Data Privacy and Protection Concerns (Web, Cloud, Mobile)****

A wide range of IoT gadgets are used for data processing, collection, leveraging, and conveying the data to premier companies. For instance, smart thermostats, smart TVs and connected printers. Thus, privacy concerns and data security is a significant concern for interconnected environments.

The user data information is sometimes sold to or distributed to different businesses. Thus, it infringes the person's right to data privacy and secrecy that escalates distrust by the public. We need to create a privacy law to protect the sensitive data information of users. We should employ similar practices for web, cloud, and mobile applications designed to manage and access the data integrated with IoT devices.

## ****Wrapping up****

It would not be wrong to say that IoT is one of the most implausible technology innovations. However, everything that connects to the internet is vulnerable to security attacks. Cybersecurity researchers and many leading companies are working their way to make it safe for IoT consumers. Yet, there is still a lot that needs to be done.