2,249 views | Sep 20, 2018, 09:00am

Five Reasons Why IoT Is Not Ready For Prime Time

Asokan Ashok Forbes Councils
Forbes Technology Council CommunityVoice

POST WRITTEN BY

Asokan Ashok

Ashok, CEO of **UnfoldLabs,** is an innovation veteran who believes in making the world a better place with futuristic technology products.

Getty

IoT as technology has been in a media hype cycle for the past few years. It has connected millions of devices, and it won't slow down anytime soon. According to Gartner, the number of IoT devices connected to the network is expected to reach 20.8 billion by 2020.

In the current state of the IoT industry, there is an abundance of technology, smart devices and innovative solutions, but there are also many issues and inflated expectations. While the benefits of IoT technology are numerous, IoT is still not ready for prime time. Here's why:

1. Fragmentation In Protocols

Over the past few years, soaring VC investments in IoT technology created plenty of media buzz, and that motivated many companies to enter the IoT race and compete for a share of the VC dollars. This influx of companies oversaturated the IoT market with new products, resulting in a fragmented landscape.

Fragmentation in protocols has become one of the issues in adopting IoT technologies and solutions on a commercial scale. It also pushed original equipment manufacturers to make devices/hubs that cannot take care of all the protocols, and it has become overwhelming to an average consumer.

Aside from the adoption challenges, the main problems of this fragmentation are the integration and interoperability issues that the consumers are facing. Due to the fragmentation of the protocols, device management has been a complex process that many consumers have not been able to address adequately. Think of having consumers doing complex operations like firmware updates, maintenance, OS updates, patches and feature rollouts -- all of which can be a nightmare due to the protocol fragmentation.

2. Power-Related Issues

Due to the cost of some IoT powered devices, OEMs are making them as small and cheap as possible. Because of this, some devices are battery powered. However, these battery-powered versions stop functioning when the batteries die. Battery technologies are having trouble keeping up with the needs of IoT devices, which has been an issue for consumers. Think of yourself buying an IoT camera with batteries and the batteries dying on you while you are on vacation.

3. Connectivity

Some of the markets worldwide have stable connections to local networks or the internet, but that's not necessarily true for the rest of the world. The challenge here is that connectivity is not universal everywhere, and because of that, IoT products and applications won’t work the way they should.

Also, the sheer number of different IoT devices creates issues. It's not unusual for the average consumer to require an expert service provider to make sure that their devices are on their network and functioning properly.

Though some of the devices are coming up with online and offline modes, the instant connectivity phenomenon and the fear of losing connectivity to the devices is an important problem for consumers. Think of smart homes or AgTech using IoT for security purposes that cannot be monitored without a connection. Another issue with connectivity is that devices are pumping the collected data into multiple clouds and cloud-based platforms, which have their own sets of restrictions and application programming interfaces.

4. Security

Given the many data breaches in the past few years, IoT security is under more scrutiny than ever. Gartner predicts that the IoT security-related spending will be $1.5 billion in 2018 and will increase to $3.1 billion by 2021.

With a surge of IoT devices in smart homes and cities, implementing security features for these devices is a need felt industrywide. However, this has not been addressed as of yet by the industry.

Research conducted by Avast (via ETCIO.com) revealed that at least 32,000 smart homes and businesses are at risk of leaking data.

Though IoT as technology has slowly matured and more products are coming our way, the security on IoT devices is still in its nascent stage. Novice hackers can easily hack these devices. A study released by Hewlett-Packard revealed that 70% of IoT devices are vulnerable to hacking.

Initial IoT developments focused on individual devices and single-purpose applications with a lack of cohesive or truly interoperable infrastructure and security. Today, every new IoT product brings in a unique connectivity and security issue that is vital to ensuring ecosystem integrity. One crucial step to address this issue is to shift away from proprietary implementations to scalable and consistent standards-based architectures that are still evolving.

On top of the device-level security, the amount of data generated and stored in SaaS- and PaaS-based platforms opens up a whole new set of data privacy and security issues. For example, data collected from an IoT-connected door can provide hackers with information about your daily movement, such as when you go on vacation or what time you come back from work. By having access to this type of data, hackers can easily predict your future movements and use these to cause damage.

5. Costs

The high costs of IoT products have significantly slowed down the mass adoption of IoT technology, which means the prices will have to drop if we want this to change. The amount of data that is being generated by the devices adds another

layer of complexity in terms of storage, and increases the total cost of ownership as well. Many companies are still trying to figure out their big data strategies, and some are moving toward smart data strategies to lower the cost of ownership of the data that is being collected and stored. Starting small, getting the needed data is the key to understand the cost implications of IoT.

In conclusion, IoT is here, but we are not ready to fully embrace it. The reasons described above are critical for IoT mass adoption, and if they are not addressed, we won't be prepared for the next wave of IoT innovations.

Here is my question to my fellow industry leaders:

How are we going to fix these above issues? Do we have a silver bullet to address the harmful side effects of hype and exponential growth of IoT?

Asokan Ashok Forbes Councils

Ashok, CEO of UnfoldLabs, is an innovation veteran who believes in making the world a better place with futuristic technology products.... **Read More**