Challenges of IoT

The Internet of Things (IoT) — a universe of connected things providing key physical data and further processing of that data in the cloud to deliver insights presents a huge opportunity and challenges for all users. This article seeks to highlight and discuss some of the challenges that are associated with IoT.

Security

IoT has already turned into a serious security concern that has drawn the attention of prominent tech firms and government agencies across the world. The hacking of baby monitors, smart fridges, thermostats, cameras and even the radio in cars are signifying a security nightmare being caused by the future of IoT. So many new devices being added to networks and the internet will provide malicious actors with many attack vectors and possibilities to carry out their evil deeds, especially since a considerable number of them suffer from many security vulnerabilities. The lack of security in IoTs is mainly due to the fact that IoT manufactures are more concerned in releasing new innovative technologies that little emphasis is focused on security.

Connectivity

Connecting so many devices will be one of the biggest challenges of the future of IoT, and it will defy the very structure of current communication models and the underlying technologies. At present we rely on the centralized, server/client system to authenticate, authorize and connect different devices in a network.

This server/client model is sufficient for current ecosystems, where thousands of devices are involved, however, when networks grow to join billions and hundreds of billions of devices, centralized systems will turn into a bottleneck. Such systems will require huge investments and spending in maintaining cloud servers that can handle such large amounts of information exchange, and entire systems can go down if the server becomes unavailable.

The future of IoT will very much have to depend on decentralizing IoT networks. Part of it can become possible by moving some of the tasks to the edge, such as using fog computing models where smart devices such as IoT hubs take charge of mission-critical operations and cloud servers take on data gathering and analytical responsibilities.

Other solutions involve the use of peer-to-peer communications, where devices identify and authenticate each other directly and exchange information without the involvement of a broker. Networks will be created in meshes with no single point of failure. This model will have its own set of challenges, especially from a security perspective, but these challenges can be met with some of the emerging IoT technologies such as Blockchain.

Compatibility and Longevity

IoT is growing in many different directions, with many different technologies competing to become the standard. This will cause difficulties and require the deployment of extra hardware and software when connecting devices.

Other compatibility issues stem from non-unified cloud services, lack of standardized machine to machine (M2M) protocols and the variations in firmware and operating systems among IoT devices.

Some of these technologies will eventually become obsolete in the next few years, effectively rendering the devices implementing them useless. This is especially important, since in contrast to generic computing devices which have a lifespan of a few years, IoT appliances (such as smart fridges or TVs) tend to remain in service for much longer, and should be able to function even if their manufacturer *goes out of service*.

Regulations

While some businesses immediately embraced the IoT, others are hesitant. In many cases, these businesses are waiting for government officials to intervene with new standards and regulations.

However, since the IoT, the cloud and even the common Internet aren't tied to one specific city, state or region, some entities question who is the responsible for these regulations.

Complicating matters even further is the sheer amount of IoT-connected devices. Since these devices originate from many different sources, including international partners and vendors, how does a localized regulatory agency control the quality of incoming shipments?

In the absence of these standards, the Internet Society has developed an Online Trust Alliance (OTA) that identifies and promotes security and privacy best practices.