WHAT'S NEXT FOR THE INTERNET OF THINGS

In 2008, the number of devices connected to the Internet surpassed the number of humans (Evans, 2011) and the trend hasn't changed much since then. While there are already a great number of devices connected to the Internet of Things, that number will only increase in the coming years. While the prospect of more interconnected devices is exciting, there are many obstacles that still remain for Electrical and Computer Engineers to overcome before the Internet of Things can reach its full potential.

The high number of potential internet-connected devices will cause problems. This may mean that current protocols and methods for connecting to the Internet no longer suffice. Additionally, all of these new devices will be generating data from the sensors at a very high rate. It will be important to store that data and to ensure that it is stored accurately, so that it is trustworthy (Stankovic, 2014).

Standard computers connect to the Internet using a protocol known as the IP (the Internet Protocol). Part of the IP puts limits on how many devices can connect to the Internet. The influx of new Internet-connected Internet of Things devices will test this limit. Fortunately, there is a new version of the IP, IPv6, which should increase this limit enough to sustain the Internet of Things (Zhou, 2013). Along with increasing the number of devices that can connect to the Internet, IPv6 will allow them to communicate faster then ever before.

IPv6 won't suffice for every Internet of Things device. The fact that many Internet of Things devices will operate on small amounts of power demands a low power alternative to IPv6. One solution to this is a technology named 6LoWPAN. Unlike IPv6, 6LoWPAN will not connect directly to the Internet. Rather it will connect to other nearby devices in what is known as a mesh network (Hersent, 2012). This technology will allow Internet of Things devices to save power while communicating with each other, but it does not prevent them from connecting to the Internet as well.

As with any software system, the Internet of Things is a target for hackers. However, unlike the traditional Internet, where a successful hacker may gain access to a social network account, hacking attacks on the Internet of Things pose a much larger risk. Where previous hackers mostly operated in the digital realm, the Internet of Things will introduce the risk of hackers operating in the physical world. The stakes are higher because these internet-connected objects will be able to collect sensitive

sensor data about their environment and may even have the power to control it, for instance by unlocking a door or disabling a security system. This problem is further complicated because Internet of Things devices will be lightweight and will require lightweight security systems that are still robust enough to do their jobs (Stankovic, 2014). Fortunately, the area of system security is an active research topic in both Computer Science and Electrical and Computer Engineering disciplines.

One such area of research involves preventing hackers from gaining unauthorized access to data. Since Internet of Things devices will be connected to the Internet, they will be exposed to the same security risks that any normal website faces. Fortunately, since these smart devices will connect to the Internet by the same means as current computers, they can use the same tried and true security measures (Ning, 2013). On top of this, any advances in computer security will also benefit Internet of Things devices.

Another area of research involves defending against attacks intended to take Internet of Things devices offline. These attacks typically are achieved in two ways. First a denial of service attack could overwhelm the device by sending it much more data than it is capable of processing. This could potentially stop it from performing its non-Internet-connected function. Second a jamming system could be used to prevent wireless devices from accessing the Internet by interfering with their wireless communications (Ning, 2013). Both of these attacks reduce the smart device's functionality, either back to that of a dumb device or even to the point where the device fails to function.

Since smart devices will know more personal data about their users than any device before, their security is a high priority for the Electrical and Computer Engineers developing them. Consumers need to be able to trust the devices and the engineers must work to preserve that trust.

Source : https://sites.tufts.edu/eeseniordesignhandbook/2015/internet-of-things/