Supplemental Reading for Internet of Things

To learn more about the "Internet of Things," click here. (or just read my copy and paste below)

Smart toasters, connected rectal thermometers and fitness collars for dogs are just some of the everyday "dumb items" being connected to the web as part of the Internet of Things (IoT).

Connected machines and objects in factories offer the potential for a 'fourth industrial revolution', and experts predict more than half of new businesses will run on the IoT by 2020.

Here's everything you need to know about the increasingly connected world.

What is the Internet of Things?
In the broadest sense, the term IoT encompasses everything connected to the internet, but it is increasingly being used to define objects that "talk" to each other. "Simply, the Internet of Things is made up of devices – from simple sensors to smartphones and wearables – connected together," Matthew Evans, the IoT programme head at techUK, says.

By combining these connected devices with automated systems, it is possible to "gather information, analyse it and create an action" to help someone with a particular task, or learn from a process. In reality, this ranges from smart mirrors to beacons in shops and beyond.

"It's about networks, it's about devices, and it's about data," Caroline Gorski, the head of IoT at Digital Catapult explains. IoT allows devices on closed private internet connections to communicate with others and "the Internet of Things brings those networks together. It gives the opportunity for devices to communicate not only within close silos but across different networking types and creates a much more connected world."

Why do connected devices need to share data?
An argument has been raised that only because something can be connected to the internet doesn't mean it should be, but each device collects data for a specific purpose that may be useful to a buyer and impact the wider economy.

Within industrial applications, sensors on product lines can increase efficiency and cut down on waste. One study estimates 35 per cent of US manufacturers are using data from smart sensors within their set-ups already. US firm Concrete Sensors has created a device that can be inserted into concrete to provide data on the material's condition, for instance.

"IoT offers us opportunity to be more efficient in how we do things, saving us time, money and often emissions in the process," Evans says. It allows companies, governments and public authorities to re-think how they deliver services and produce goods.

"The quality and scope of the data across the Internet of Things generates an opportunity for much more contextualised and responsive interactions with devices to create a potential for change," continued Gorski. It "doesn't stop at a screen".

The latest Internet of Things news

Where does the IoT go next?

Even those who have purchased one of the myriad smart home products – from lightbulbs, switches, to motion sensors – will attest to the fact IoT is in its infancy. Products don't always easily connect to each other and there are significant security issues that need to be addressed.

A report from Samsung says the need to secure every connected device by 2020 is "critical". The firm's Open Economy document says "there is a very clear danger that technology is running ahead of the game". The firm said more than 7.3 billion devices will need to be made secure by their manufacturers before 2020.

“We are looking at a future in which companies will indulge in digital Darwinism, using IoT, AI and machine learning to rapidly evolve in a way we’ve never seen before," Brian Solis, from Altimeter Group, who helped on the research said.

IoT botnets, created using a network of out-of-date devices took large websites and services offline in 2016. A Chinese firm later recalled 4.3 million unsecured connected cameras. The ease of bringing down the internet using IoT devices was revealed when instead of malicious purposes, the botnet was revealed to have been created to game Minecraft.

But aren't there privacy implications?

Everything that's connected to the internet can be hacked, IoT products are no exception to this unwritten rule. Insecure IoT systems led to toy manufacturer VTech losing videos and pictures of children using its connected devices.

There's also the issue of surveillance. If every product becomes connected then there's the potential for unbridled observation of users. If a connected fridge tracks food usage and consumption, takeaways could be targeted at hungry people who have no food. If a smartwatch can detect when you're having sex, what is to stop people with that data using it against the watches' wearer.

“In the future, intelligence services might use the [internet of things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials,” James Clapper, the US direction or national intelligence said in 2016. Wikileaks later claimed the CIA has been developing security exploits for a connected Samsung TV.

We need reliable standards

At the centre of creating a vast, reliable IoT network lies one significant issue: compatible standards. Connected objects need to be able to speak to each other to transfer data and share what they are recording. If they all run on different standards, they struggle to communicate and share. The Institute of Electrical and Electronics Standards Association lists a huge number of standards being developed and worked on for different applications.

"Additional needs are emerging for standardisation," the Internet Society says. If standardisation happens it will let more devices and applications be connected.

To try and tackle this issue on an enterprise scale, Microsoft has introduced its own system for IoT devices. Called IoT Central, TechCrunch, reports the system gives businesses a managed central platform for setting up IoT devices. Microsoft claims the system will simply the creation of IoT networks.

Gorski described IoT, even among those with the most experience of the concept, as a "relatively immature market" but said 2016 may have been a turning point. The Hypercat standard is now supported by ARM, Intel, Amey, Bae Systems and Accenture and the firms are currently agreeing on a format for "exposing collections" of URLs, for example.

"In the short term, we know [IoT] will impact on anything where there is a high cost of not intervening," Evans said. "And it'll be for simpler day-to-day issues – like finding a car parking space in busy areas, linking up your home entertainment system and using your fridge webcam to check if you need more milk on the way home.

"Ultimately what makes it exciting is that we don't yet know the exact use cases and just that it has the potential to have a major impact on our lives."

This article was originally published in march 2023 It has since been updated with further IoT information.

Heads up: A big part of being successful in an IT role is the ability to be a self-led learner -- someone who finds key resources and reads up on the latest tech trends and solutions. The supplemental readings we've provided have been designed to show you just some of the support materials available to you online; they're not meant to be considered a comprehensive list. Feel free to add to the conversation by posting other useful resources for learners to this forum thread.

Revision #1
Created 2023-05-29 12:52:23 UTC by naruzkurai
Updated 2023-05-29 13:09:07 UTC by naruzkurai