What is the dark side of IoT?

Published on 7 Jan 2020

As we surpass 2019, it's high time we realise that by merging the digital and physical realm, IoT is destined to change the way we live and work.

I have always been interested in the intersection between business and technology, and today it seems that the brave new technological world we have been dreaming over centuries has arrived. With everything from home appliances to smart vehicles, portable devices are connected to the internet and exchange crucial data. According to the statistics, there are 26.66 billion IoT connected devices around the globe. Which statistically leaves every citizen of the world with at least 3 devices.

IoT in every day life
I must say the numbers are quite mind-boggling! And this leaves a lot of room for improvement by incorporating the Internet of Things in software development; whether it’s a mobile app or web. According to the statistics, there are 26.66 billion IoT connected devices around the globe. Which statistically leaves every citizen of the world with at least 3 devices. It may interest you to know that the Internet of Things has the potential to touch every domain and nearly every aspect of human life. According to sources, impact on IoT leads to:

- By 2020, 50 billion devices are expected to connect to the internet.
- In 2015, 3.5 connected devices per person have now reached almost 7.
- 8 billion mobile broadband access points by 2019.
- 5 million IoT jobs by 2020.
- 70 percent a year growth through 2018 in total sales of clothing and accessories incorporating computer technology, rising from $3 billion today to $42.5 billion.
- $3.3 trillion market for ‘Smart City’ applications and services by 2025.

The impact of smart homes

Instead of saying the home is where our heart is; a home is where a bot is. However, IoT hasn’t entirely arrived in our homes. I mean, we are still required to order groceries the minute we run out of eggs and Greek yogurt. Slowly and steadily we are getting there; it seems the latest advancements in artificial intelligence and big data analytics will definitely work wonders for us. Smart homes are no longer a dream project; we can soon expect everything to be governed by the “brain” or a central platform. Moreover, bots will be seen tackling a certain set of functions related to more difficult tasks, and lastly niche bots, in charge of single tasks such as vacuuming the house or addressing more complex duties like accounting, coaching or household managing. Tech giants, or should I call them current development frontrunners like Amazon, Google,
Samsung and Apple are expected to come up with something nerve-cracking.

The benefits of IoT

Other than this, with IoT, you will be able to work smarter and not harder. Artificial intelligence and advanced analytics can help create a more intelligent work environment. For example, the right AC temperature in shared office spaces help us book the most convenient meeting room, and moreover, take into account the room preference by setting the right temperature, lighting, and can automatically restock office supplies.

This simply leads to:

- More efficient office operations
- Energy savings
- Comfortable work environments
- Consequently increased employee productivity
- The dark side of the Internet of Things

The potential risks

Every technology indeed comes as a boom, but that doesn’t mean the grass will be greener on the other side. Furthermore, we will uncover how even after offering so much convenience why IoT poses so much risk. Like I said before, IoT can be integrated into anything from coffee machines to fitness watches leading to make our lives more convenient. But what happens if they turn bad? When being unwillingly infected or hacked, these blessings can certainly turn into huge threats.

Devices, systems and the lack of security

It may interest you to know that IoT devices can become bots that blindly follow commands to commit crimes as part of a botnet. What is a botnet, you may ask? Well, it is a network of
infected devices that are mainly abused by the attacker to perform tasks such as carrying out DDoS attacks, Bitcoin mining and spreading spam emails. Mainly being used to carry out DDoS attacks and to mine for cryptocurrencies, these botnets have the potential to have a larger impact by making IoT devices do much more, such as send spam messages featuring dangerous malware. Botnets can also carry out click-jacking campaigns, distribute fake advertisements, and even worse, infect other IoT devices.

"Botnets can also carry out click-jacking campaigns, distribute fake advertisements, and even worse, infect other IoT devices"

Much like most malware, botnets can be found on dark marketplaces. The source code can be purchased and leaked, depending on the type of service. In case, an IoT device is already infected, another bot can attempt to replace the infection with its code and in some cases also "repair" the security vulnerability. But most of the time it fails! No matter how innocent these proof-of-concept attacks may seem, one cannot deny the fact that IoT devices and systems aren't properly secured. Hackers can easily gain control of them and cause complete chaos like never before.

Collecting information at a cost

But how much information can an IoT device collect? What I mean is that by hacking a webcam, one can see what they are pointed at without you even knowing it, smart TVs and personal assistants can pick up sound, and smart cars can give clues to whether or not someone is home. Honestly, the amount of information collected on these IoT devices cannot be determined at any cost. And with everything in the cloud, such information can be intercepted or rerouted to a malicious server and be abused if not properly secured.

The more we surround ourselves with IoT devices, the more motivation cybercriminals receive to target us! With the time passing by, let’s simply hope that connected device security will dramatically improve.

Author Profile
Charles Richard
You may also be interested in...

**Shifting focus: Internet of Things (IoT) from the security manufacture...**

The term Internet of Things (IoT) has almost been beaten to death at this point, as more and more security integrators, manufacturers and cu...

**How Internet of Things (IoT) aids facility management and physical sec...**

As buildings become more complex and smarter, the age-old traditional maintenance methods that are based mostly on hands-on human monitoring...

**Video technology reimagined with the empowerment of IoT**

It amazes me how in a few short years security systems have gone from simple, dumb cameras witnessing events to intelligent eyes, ears, spee...

**Unifying the mobile experience: cloud, IoT and the AI evolution of acc...**

The industry faces numerous challenges in the coming year. Physical and cyber security threats continue to become more complex, and organisa...