IJCSN - International Journal of Computer Science and Network, Volume 8, Issue 2, April 2019
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Internet of Things Today Computer World

[1] Navneet Sandhu; [2] Sheilly Padda; [3] Umesh Sehgal

[1, 2, 3] Chandigarh Engineering College, Landran

Abstract - "Today computers and, therefore, the internet are almost wholly dependent on human beings for information. Nearly all of the roughly 50 petabytes (a petabyte is 1,024 terabytes) of data available on the internet were first captured and created by human beings by typing, pressing a record button, taking a digital picture or scanning a bar code. The problem is, people have limited time, attention and accuracy all of which means they are not very good at capturing data about things in the real world. If we had computers that knew everything there was to know about things using data they gathered without any help from us we would be able to track and count everything and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling and whether they were fresh or past their best."

Keywords - *IoT Security Tools*

1. Introduction

A thing, in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low -- or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network.

IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS), microservices and the internet. The convergence has helped tear down the silo walls between operational technology (OT) and information technology (IT), allowing unstructured machine-generated data to be analyzed for insights that will drive improvements.
The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

A thing, in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low -- or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network.

IoT has evolved from the convergence of wireless technologies,
Micro-electromechanical systems (MEMS), microservices and the internet. The convergence has helped tear down the silo walls between operational technology (OT) and information technology (IT), allowing unstructured machine-generated data to be analyzed for insights that will drive improvements.

Kevin Ashton, cofounder and executive director of the Auto-ID Center at MIT, first mentioned the Internet of Things in a presentation he made to Procter & Gamble in 1999. Here's how Ashton explains the potential of the Internet of Things:

IPv6's huge increase in address space is an important factor in the development of the Internet of Things. According to Steve Leibson, who identifies himself as "occasional docent at the Computer History Museum," the address space expansion means that we could "assign an IPV6 address to every atom on the surface of the earth, and still have enough addresses left to do another 100+ earths." In other words, humans could easily assign an IP address to every "thing" on the planet. An increase in the number of smart nodes, as well as the amount of upstream data the nodes generate, is expected to raise new concerns about data privacy, data sovereignty and security.

Practical applications of IoT technology can be found in many industries today, including precision agriculture, building management, healthcare, energy and transportation. Connectivity options for electronics engineers and application developers working on products and systems for the Internet of Things include:

Although the concept wasn't named until 1999, the Internet of Things has been in development for decades. The first internet appliance, for example, was a Coke machine at Carnegie Melon University in the early 1980s.

The programmers could connect to the machine over the internet, check the status of the machine and determine whether or not there would be a cold drink awaiting them, should they decide to make the trip down to the machine.

Advantages and Disadvantages of IoT

IoT is tagging our day-to-day objects with machine-readable identification tags. Sensors may be a couple with these tags to collect more information about the condition the everyday objects and those present around them.

The time is not that far when you are out of home and your computers at home contact you to let you know that your medicines have expired or that the milk is over or you need more pepper. This isn't just a fantasy but soon to be a reality due to the amazing possibilities of the Internet of Things (IoT).IoT is tagging our day-to-day objects with machine-readable identification tags. Sensors may be a couple with these tags to collect more information about the condition the everyday objects and those present around them. The same applies to various companies wherein the computers would keep track of the stock available and resources and maintain them to optimum levels, thus saving a lot of time and money.

Before we understand the impact IoT can have on our way of living, it's important to go through its advantages and disadvantages:

Advantages

Here are some advantages of IoT:
1. **Data**: The more the information, the easier it is to make the right decision. Knowing what to get from the grocery while you are out, without having to check on your own, not only saves time but is convenient as well.
2. **Tracking**: The computers keep a track both on the quality and the viability of things at home. Knowing the expiration date of products before one consumes them improves safety and quality of life. Also, you will never run out of anything when you need it at the last moment.
3. **Time**: The amount of time saved in monitoring and the number of trips done otherwise would be tremendous.
4. **Money**: The financial aspect is the best advantage. This technology could replace humans who are in charge of monitoring and maintaining supplies.

Disadvantages
Here are some disadvantages of IoT:
1. **Compatibility**: As of now, there is no standard for tagging and monitoring with sensors. A uniform concept like the USB or Bluetooth is required which should not be that difficult to do.
2. **Complexity**: There are several opportunities for failure with complex systems. For example, both you and your spouse may receive messages that the milk is over and both of you may end up buying the same. That leaves you with double the quantity required. Or there is a software bug causing the printer to order ink multiple times when it requires a single cartridge.
3. **Privacy/Security**: Privacy is a big issue with IoT. All the data must be encrypted so that data about your financial status or how much milk you consume isn't common knowledge at the work place or with your friends.
4. **Safety**: There is a chance that the software can be hacked and your personal information misused. The possibilities are endless. Your prescription being changed or your account details being hacked could put you at risk. Hence, all the safety risks become the consumer's responsibility.

2. Problems in IoT

Security is a crucial issue on the Internet, and it is probably the most significant challenge for the IoT. When you increase the number of connected devices, the number of opportunities to exploit vulnerabilities through poorly designed devices can expose user's data to theft, especially when the data streams are left with inadequate protection. In certain cases, it may even harm the safety and health of people. The Zika virus is not the only threat out there!

There are a number of IoT deployments that also have collections of near identical or identical devices. This magnifies the impact of any one security vulnerability by the number of devices that all have similar characteristics.
To deal with all these unique challenges, there is a need for collaborative approach to security. A lot of users are ultimately going to have to compare the cost against the security, which is related to the mass scale deployment of the Internet of Things devices.

3. Conclusion

The future IoT will require significant changes in supporting infrastructure to accommodate the increased number of addressable sensors and devices, and the diversity in how those devices communicate. It is however unclear what architectural changes will occur, since relevant interoperability guidelines, communication standards, and vendor designs are still immature. The main benefits of autonomous capabilities in the future IoT is to extend and complement human performance. Robotic

manufacturing and medical nanobots may be useful; however, devices (including robots) run software created by human. The danger of the increased vulnerabilities is not being addressed by security workers at the same rate that vendors are devoting time to innovation. Consider how one might perform security monitoring of thousands of medical nanobots in a human body.

The Internet of Things is, at the same time, providing extraordinary value while significantly increasing security vulnerabilities. There are many factors contributing to the risk, beyond the simple explosion in volume of usage. The IoT ecosystem is very complex, especially when platforms interoperate across different technologies at every layer of the stack (chips, devices, OS, network protocols, transport, applications, standards, and more). These complexities coupled with the cost of prevention are often cited as primary reasons for increasing security risks. While these factors have merit, a fundamental difference is that IoT is increasingly controlling devices that can cause great harm if exploited (vehicles, health devices, machinery, etc.). The potential negative impact can be tragic. Fortunately, security professionals do have weapons at their disposal and the economics are moving in their favor. Component costs traditionally have been high but are becoming more economical. The IEEE 802.15.4 standard was created for use in residential and industrial markets. The more rapid proliferation of IoT in the industrial market has driven production costs down for necessary components (radio chipsets, microcontrollers, etc.).

While this allows the residential segment to take advantage of the added cost benefits of proven technology, this also adds pressure to partners within the ecosystem to stay competitive. Unfortunately, the area that has suffered from cost cutting is device and end-to-end platform security. Encryption needs computational power, which requires hardware, which in turn adds cost.

Helping to review the paper Mr Umesh Sehgal, GNA University, Phagwara.

Reference

[1] https://e27.co/advantages-disadvantages-internet-things-20160615/
[2] https://www.linkedin.com/.../pros-cons-internet-things-iot-bhaskara-reddy-sannapured..
[3] https://www.buzzle.com/articles/pros-and-cons-of-internet-of-things-iot.html
[4] https://www.networkworld.com/article/3166106/internet-of-things/4-critical-security-challenges-facing-iot.html
[5] https://www.researchgate.net/.../307873475_In_Conclusion_The_Future_Internet_of
[6] https://link.springer.com/content/pdf/10.1007/978-3-319-32125-7_16.pdf
[7] https://www.linkedin.com/.../iot-wireless-security-vulnerabilities-solutions-conclusion