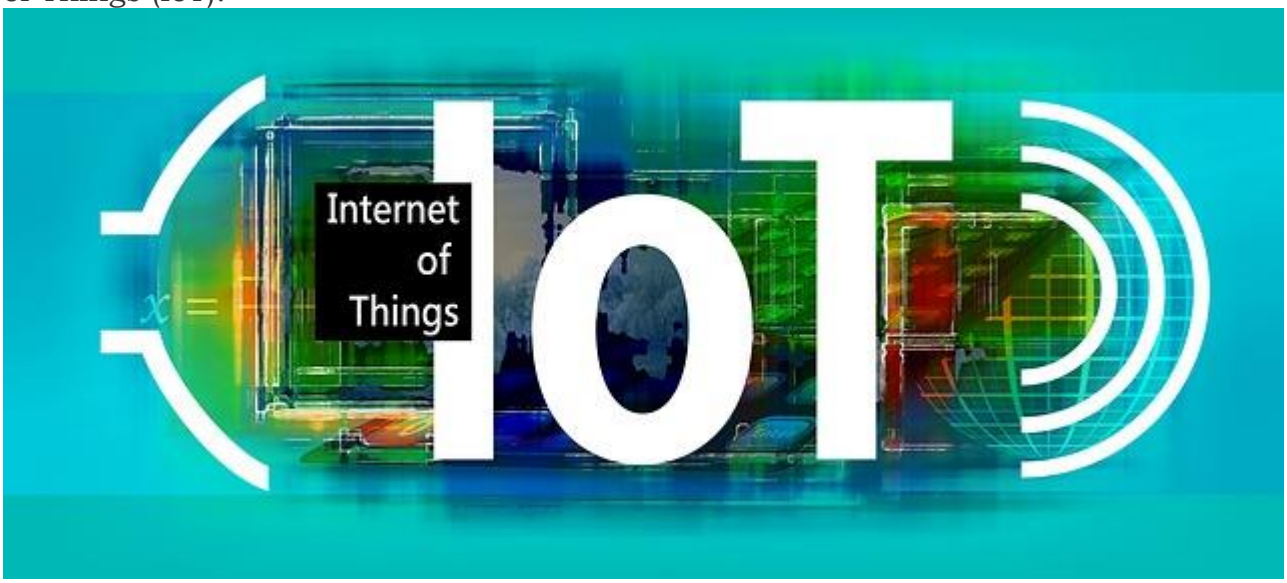
Unit 20. Internet of Things (IoT) – A Simple Explanation

Who orders vegetables for your home? You or your parents do that, right? But what if tomorrow, your *refrigerator* directly orders for vegetables after analysing the shortage in stock? Yes, that is possible with the emergence of a new concept called the Internet of Things (IoT).



What is the "Internet of Things (IoT)"?

The internet of things (IoT) is a concept that describes the idea of everyday physical objects being connected to the internet. In the Internet of Things, the connected devices should be able to identify themselves to other devices.

Simply put, this is the concept of basically connecting any device with an ON and OFF switch to the Internet or to each other. This includes everything from cell phones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of.

Or, if you want us to make it more simple – Internet of Things (IoT) is a concept where **Things can talk to other Things!**

Internet of Things – Example

Let's go back to my morning and there I am lying blissfully asleep or so it seems.

*The **sensors in my arm** sent something is very wrong my heart rate – it is going up, my breathing has become erratic, and instead of this time gently waking me, it vibrates aggressively to get my attention, and as I roll over, I I'm grabbing my chest, and I'm I'm like what's going on, so I reach over to **my phone**.*
I pull it up and sure enough there's a message it says I'm having high blood pressure in my breathing as a radicand and it suggests that I take a two aspirin right away and then goes on to say it says all my vital signs have been recorded in electronically transmitted to my medical provider.

*So back at the hospital **the doctors already evaluating my data** and in his professional opinion I need to get in the hospital right away so we electronically dispatch **Emergency Medical Team** directly to my home including pertinent data about my current medical situations so they know how to take care of me and I even get a notice or a message from the EMT that they're about to arrive I'm whisking to the hospital and I'm put under keen observation.*
*The good news is later that morning that doctor comes and says you're going to be fine. **You were suffering a heart attack** and we avoided any major damage because you got the treatment you needed in just the nick of time so now is the **internet of things** worth it maybe all **because things can talk to other things** or what we call the Internet of Things Thank you.*
Note: This is an excerpt from the speech by Benson Hougland at TEDxTemecula.

Who coined the term the Internet of Things?

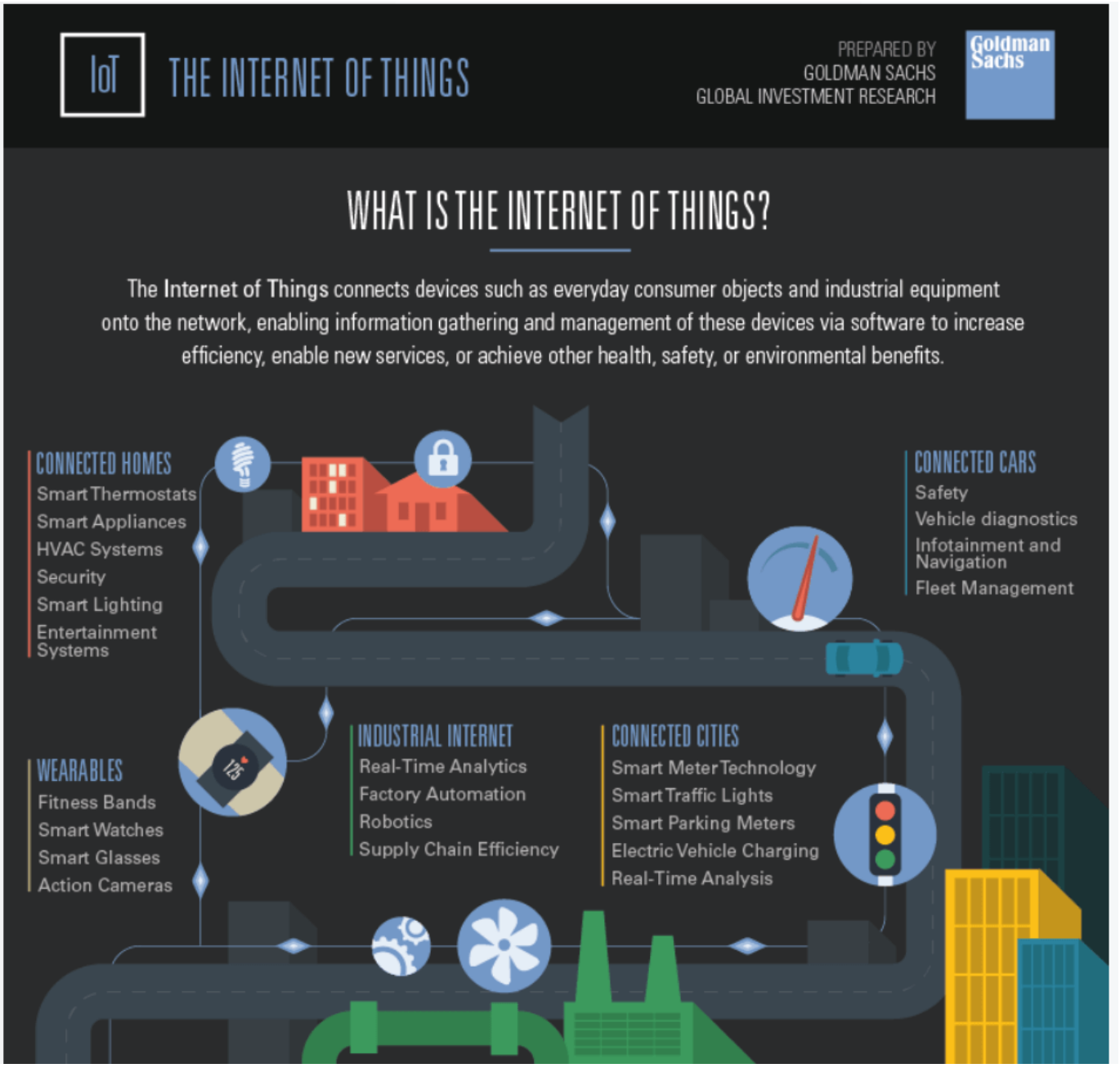
In 1999 Kevin Ashton, then at P&G (later MIT's Auto-ID Center), coined the term 'Internet of Things'. It was a new term, but not a new operation. It was known as pervasive computing, ubicomp, and ambient intelligence.

The first version of the internet was about data created by the internet. The next version is about the data created by things.

Which devices can be part of IoT?

Anything that can be connected, will be connected.

Any device, if it has an on and off switch then chances are it can be a part of the IoT. Very often the connected devices will have an I.P address. With Internet Protocol Version 6 (IPv6), assigning an IP address to billions of devices has become very much feasible.



Examples of 'things' which can be connected to internet include:

- Connected Wearables – Smartwatches, Smart glasses, fitness bands etc.
- Connected Homes – connecting household appliances to the network.
- Connected Cars – vehicles that are connected to the internet.
- Connected Cities – smart meters which analyse usage of water, gas, electricity etc connect cities to IoT

Operationally this means that we can define the Internet of Things as the seamless flow between the –

- BAN (body area network): **wearables**,
- LAN (local area network): **smart home**,

- WAN (wide area network): **connected car**, and
- VWAN (very wide area network): **the smart city**.

Key to this flow is having control of the data.

That is why Google is offering a Glass and a Lens so you can synchronize your health data into the NEST and the Google Car throughout the smart city applications of google.org. The idea is that in consumer applications and services you never have to leave the Google Cloud. The products are gateways linking up the networks.

Why would we want an Internet of Things?

We want it because it can offer us –

- the best possible feedback on physical and mental health.
- the best possible resource allocation based on real-time monitoring.
- best possible decision making on mobility patterns.
- the best possible alignments of local providers with global potential.

IoT – Opportunities and Benefits

IoT offers us the opportunity to be more efficient in how we do things, saving us time, money and often emissions in the process.

Internet of Things can be used to tackle 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.

IoT offers many other benefits industrially, such as:

- **Unprecedented connectivity:** IoT data and insights from connected applications and devices empower organizations with the ability to deliver innovative new products and services faster than their competitors.
- **Increased efficiency:** IoT networks of smart and intelligent devices provide real-time data to arm employees with the information they need to optimize their day-to-day efficiency and productivity.
- **Cost savings:** IoT devices provide accurate data collection and automated workflows to help organizations reduce their operating costs and minimize errors.
- **Time savings:** Connected smart devices can help organizations enhance the performance of systems and processes to save time.

IoT – Threats and Challenges

There is a very clear danger that technology is running ahead of the game.

More than 7 billion devices will need to be made secure by their manufacturers before 2020.

The need to secure every connected device by 2020 is “critical”.

IoT botnets, created using a network of out-of-date devices took large websites and services offline in 2016.

Everything that’s connected to the internet can be hacked, IoT products are no exception to this unwritten rule. (Remember the car hacking scene in the ‘Fate of the Furious’ movie).

If every product becomes connected then there's the potential for unbridled observation of users. This will create a lot of privacy issues.
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.

Summary

Simply, the Internet of Things is made up of devices – from simple sensors to smartphones and wearables – connected together.

IoT is increasingly being used to define objects that "talk" to each other.

IoT is a giant network of connected "things" (which also includes people). The relationship will be between people-people, people-things, and things-things.

Companies are using IoT, AI and machine learning to rapidly evolve in a way we've never seen before