

A decorative background pattern of light blue circuit board traces and nodes, resembling a network or data flow, is visible on the left and right sides of the slide.

A Brief Introduction to the Internet of Things (IoT)

Toastmasters – ACS Technical Presentations, Project # 5

Manasseh Katz, CC – 1/4/2017

What is IoT?

The **internet of things** is the internetworking of physical devices, vehicles, buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

Everything electronic, everywhere, is connected together.

Examples of IoT Devices

Consumer:

Cars, phones, appliances, thermostats, lighting, cameras, doorbells, locks, remote health monitoring



Examples of IoT Devices

Commercial/Industrial:

Power plants, utility meters, factory automation, pipeline and other remote system monitoring, vending machines, security cameras, environmental monitoring & control, access control...and much more



Why does IoT matter?

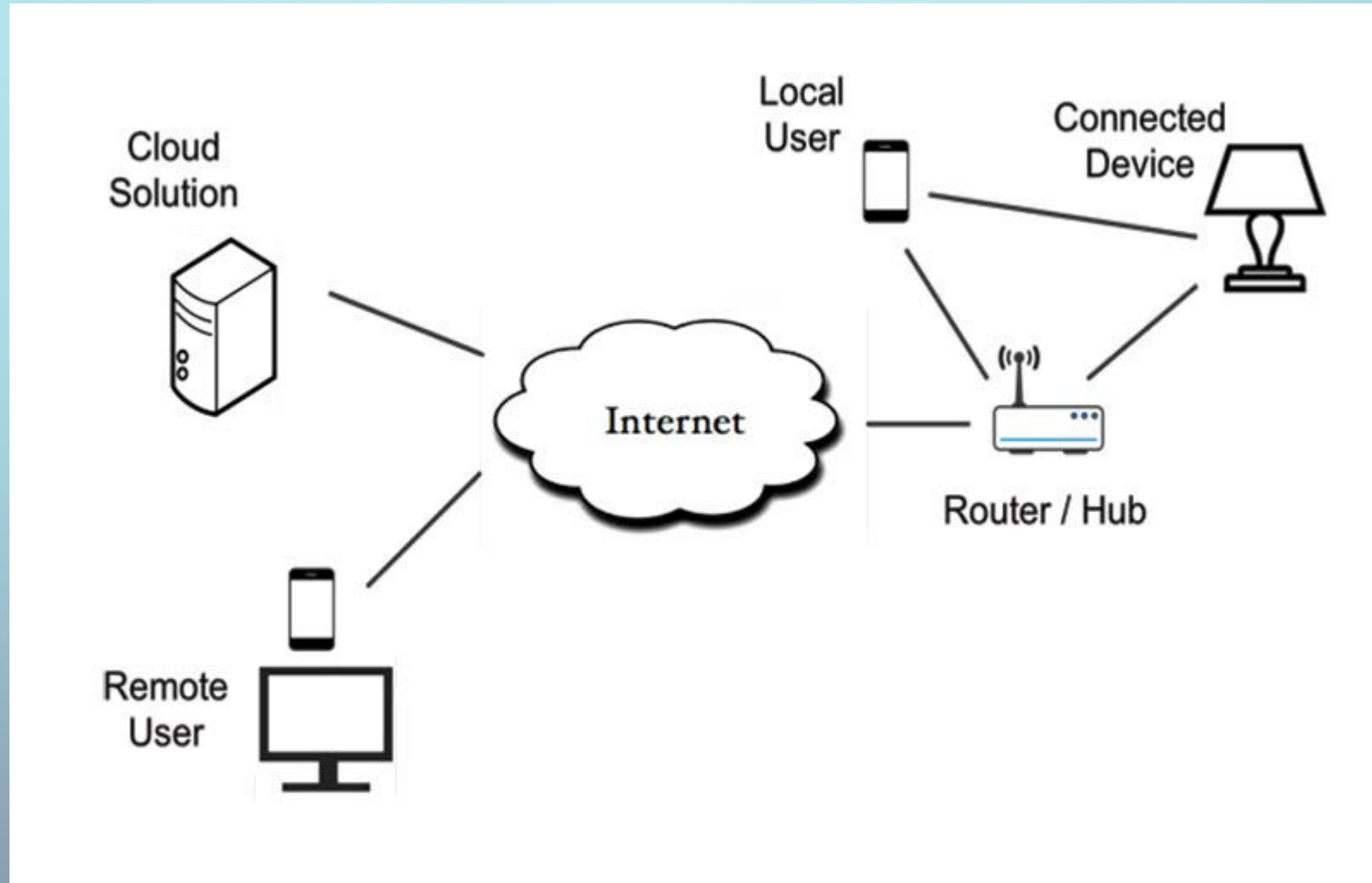
Market is huge! By 2020 estimates of 20 billion - 30 billion devices, ~ trillion dollars per year estimated market.

Productivity: More effective use of facilities & equipment; increased automation

Energy Savings: Peak demand management; intelligent environmental controls

Safety & Security: Improved access control and loss prevention at every level – home, retail, business, industrial, government & military

How does IoT work?



How does IoT work?

Intelligence: Each device needs to have a computer. These keep getting smaller and cheaper – Raspberry Pi, Arduino – and some systems are much smaller.

Communications:

IPV4 (4 billion) vs. IPV6 (3.403 x 10³⁸)

Wireless WiFi, ZigBee, Bluetooth, LTE

Wired Ethernet, PoE, power line, fiber optic

Power:

Electric Utility

Batteries – Rechargeable

Solar/alternative power

Ambient Power Harvesting – radio, motion, etc.

How does IoT work?

Input:

Human input – keypad, touch screen, voice
Sensors – mechanical, temperature, motion
Cameras

Computation:

Determine what data needs to be sent and when
Analyze & summarize data to minimize communication costs (time and \$)

Communication:

Events – changes in environment, user requests, alarms
Streaming data – audio, video
Periodic data – e.g., 15-minute meter readings

Output:

Displays similar to ordinary computers
Adjust other equipment – HVAC, lighting, machinery
Local alarms/notifications
Access Control

Problems/Challenges

Privacy: Lots of data is collected. Who can see it and what can they do with it?

Unauthorized Access (a.k.a. Hacking):

Need security for the devices and for the data in-transit.

Potential for unauthorized users to affect operation of any connected equipment.

Unauthorized users can use “open” devices to attack the internet – e.g., Mirai botnet – this has already happened.

The Future...

Autonomous Vehicles + IoT => Safer & faster travel (but harder to “escape”)

Wearable/Implanted Medical Devices + Always-on Communications => Instant diagnosis and treatment (but beware of “hackable people”)

RFID + Scanners => Never lose your car keys (or any other valuable) (but can't hide your stuff)

A Brief Introduction to the Internet of Things (IoT)

Questions?

wp.smartcomputerinc.com/iot

Toastmasters – ACS Technical Presentations, Project # 5

Manasseh Katz, CC – 1/4/2017