SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A++' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

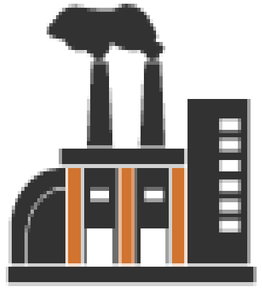
19ECT213- IoT SYSTEM ARCHITECTURE

II B.E. ECE / IV SEMESTER

UNIT 1 – BASICS OF IoT

TOPIC 1 –Introduction to IoT

REVOLUTION



1st

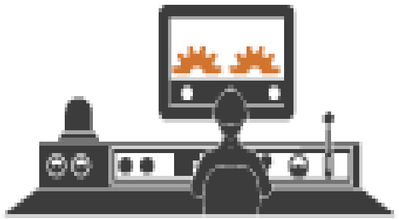
1760s

Steam engine
Mechanization

2nd

1870s

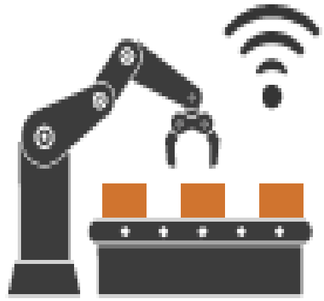
Electricity
Mass production



3rd

1960s

Computers
Automation
Internet



4th

NOW

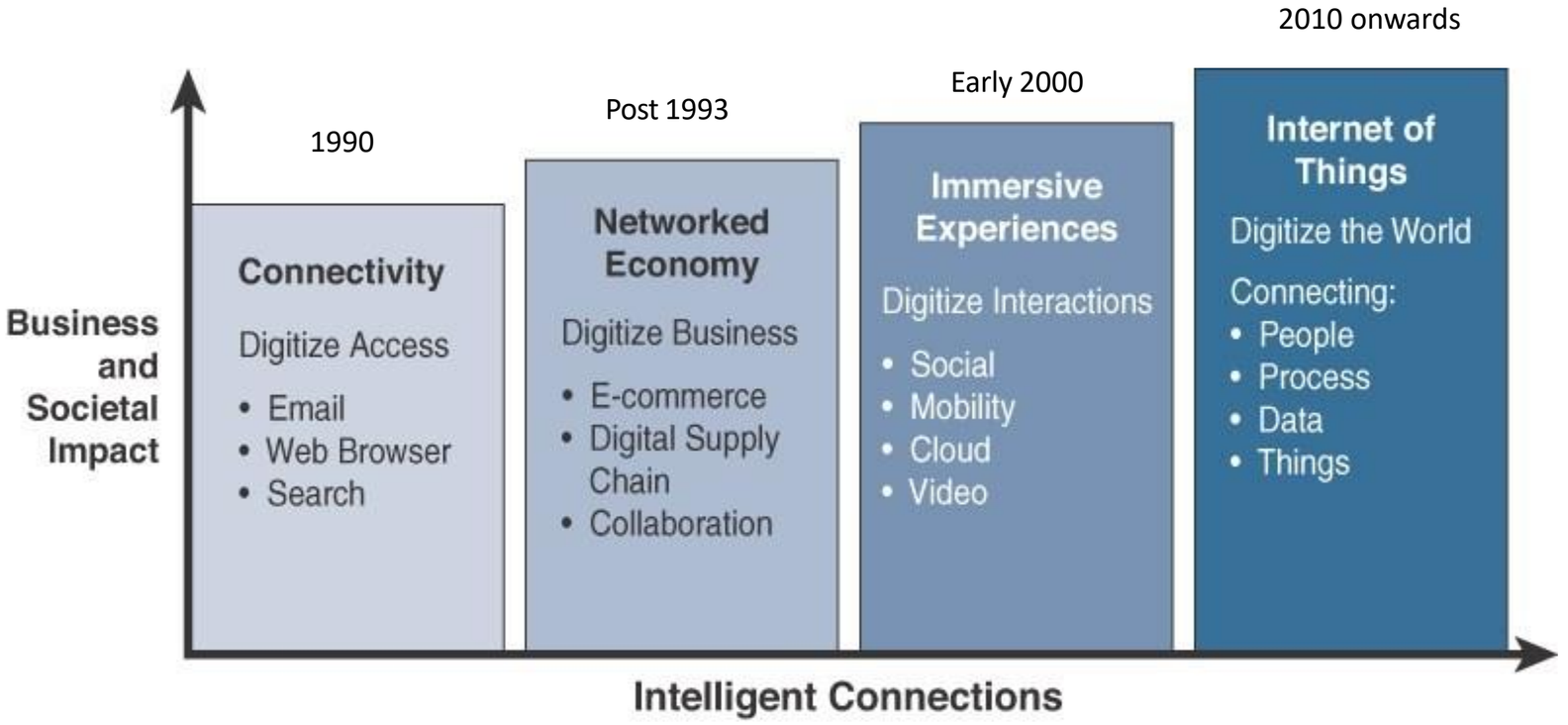
Hyper-connectivity

HISTORY OF IOT

- 1970- The actual idea of connected devices was proposed
- 1990- John Romkey created a toaster which could be turned on/off over the Internet
- 1995- Siemens introduced the first cellular module built for M2M
- 1999- The term "Internet of Things" was used by Kevin Ashton during his work at P&G
- 2004 - The term was mentioned in famous publications like the Guardian, Boston Globe, and Scientific American
- 2005-UN's International Telecommunications Union (ITU) published its first report on this topic.
- 2008- The Internet of Things was born
- 2011- Gartner, the market research company, include "The Internet of Things" technology in their research

Evolutionary Phases of the Internet

- The popularity of the term IoT did not accelerate until 2010/2011 and reached mass market in 2013-14.
- Definition of the IoT has evolved over time.



What is IOT?

- ✓Internet of Things (IoT) is the **network of smart physical objects**
  - physical objects (e.g. devices, vehicles, buildings, etc.) embedded with sensors/actuators, computation unit, memory unit, power source, and network connectivity,
  - which enables the physical object to collect and exchange data,
  - analyze the collected data to extract new insight and respond accordingly.

- ✓Goal of IoT is to "connect the unconnected"
  - "Things" or "objects" that were not supposed to be connected to the Internet
  - IoT did the technology transition in traditional computer networks

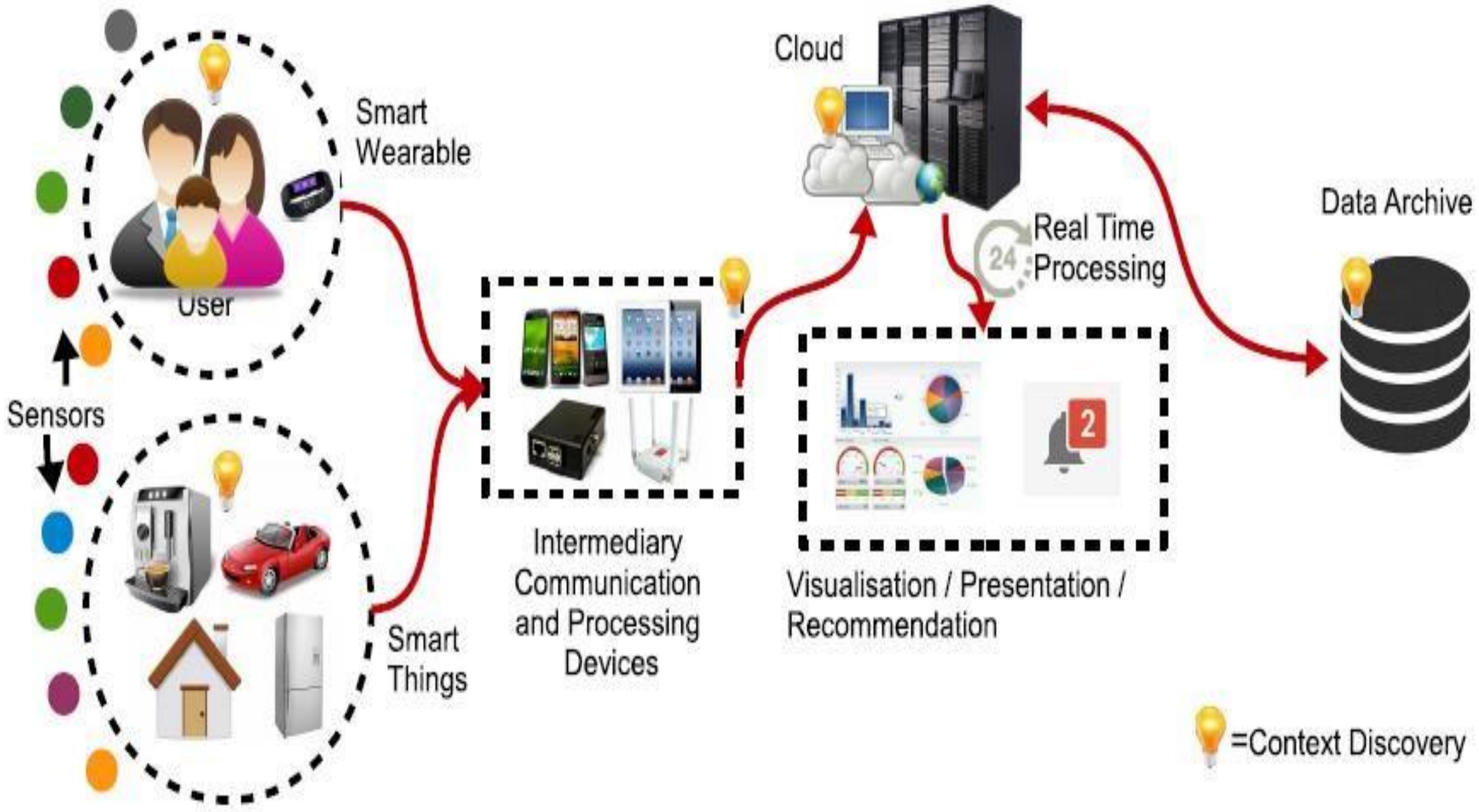
What is IOT?

- IoT is a concept of connecting any device with an on and off switch to the Internet (and/or to each other).
- This includes everything from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of.
- This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig – Forbes.
- The IoT is a giant network of connected "things" (which also includes people). The relationship will be between people-people, people-things, and things-things.
- The dominant consumer IoT device, worldwide, is the smart TV. Between 25-35% cent of consumers worldwide own a television that can connect to the Internet, according to a Deloitte research. However, other areas of the IoT market are growing rapidly.

What is IOT?

- An IoT ecosystem consists of web-enabled smart devices that use embedded processors, sensors and communication hardware to collect, send and act on data they acquire from their environments.
- IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analyzed or analyzed locally.

IoT ecosystem

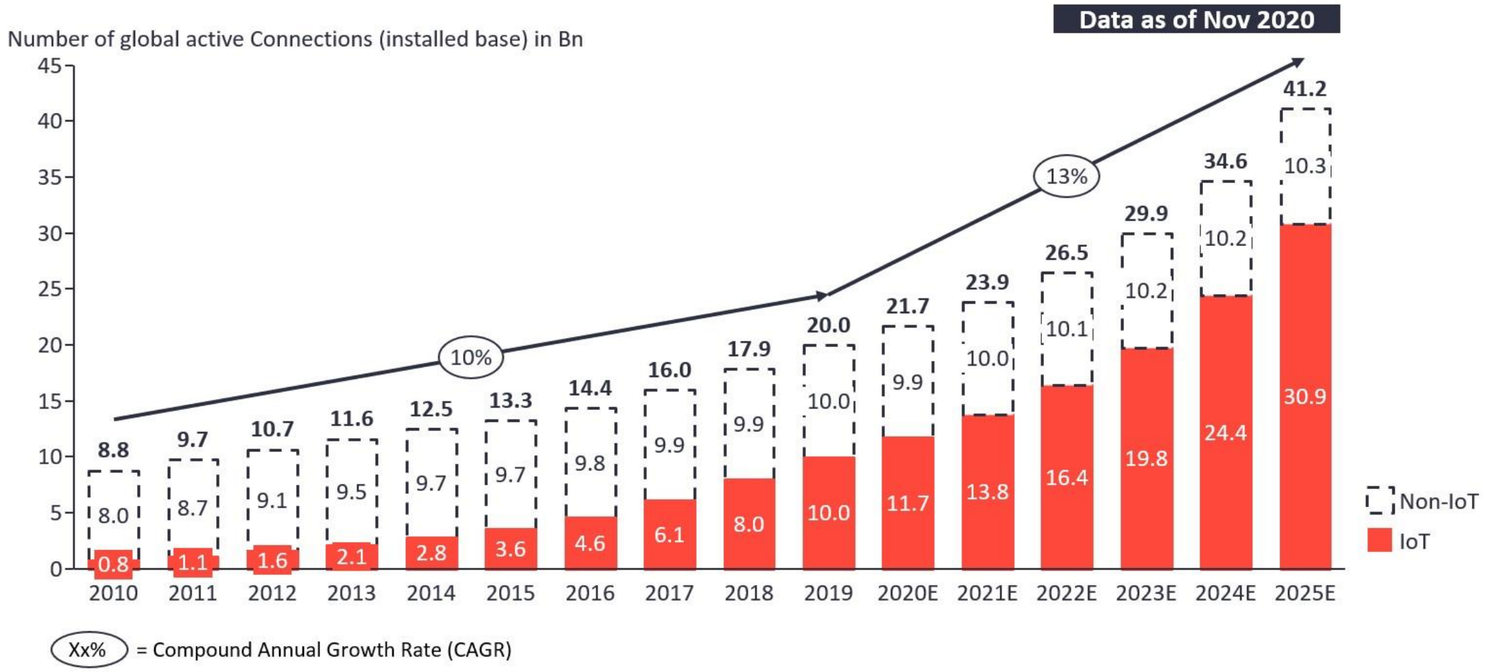


IMPACT OF IOT

Growth of IOT Devices

Total number of device connections (incl. Non-IoT)

20.0Bn in 2019– expected to grow 13% to 41.2Bn in 2025

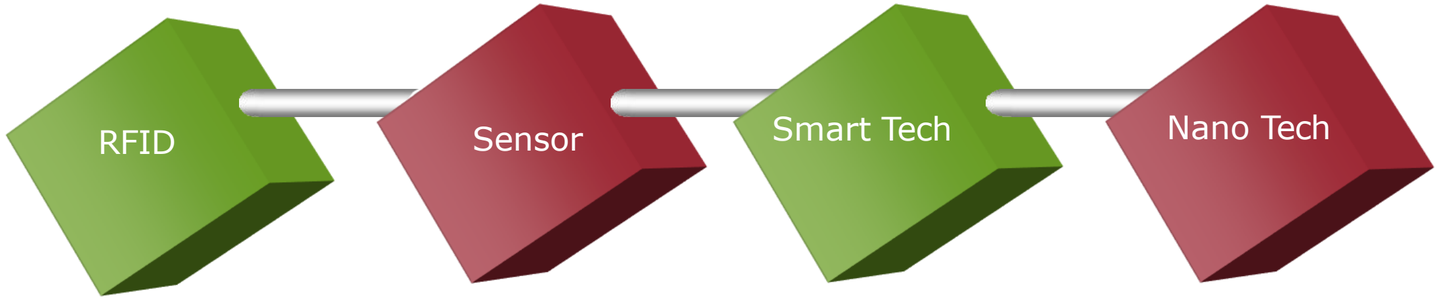


Note: Non-IoT includes all mobile phones, tablets, PCs, laptops, and fixed line phones. IoT includes all consumer and B2B devices connected – see IoT break-down for further details

Source(s): IoT Analytics - Cellular IoT & LPWA Connectivity Market Tracker 2010-25

ACTIVITY TIME!

HOW IOT WORKS



To identify and track the data of things	To collect and process the data to detect the changes in the physical status of things	To enhance the power of the network by devolving processing capabilities to different part of the network.	To make the smaller and smaller things have the ability to connect and interact.

BENEFITS OF IOT

- Automation
  - Machines can assemble parts with more precision and speed, resulting in fewer errors during assembly
  - Robots can very rapidly detect faults that may not be detected by the human eye
- Predictive Maintenance
  - Continuous monitoring of systems and processes to identify key indicators of problems before they result in downtime or system failure
- Process / Efficiency Improvement
  - Process improvement affects every aspect of an operation's bottom line
- Cost Reduction
  - When an organization can improve system uptime, automate processes, reduce the risk of failure and gain insights that support better decision making, and reduce resource usage, the result is efficiency and cost savings
- Improved/ New Insights
  - IoT systems often act as the eyes and ears on remote, hard-to-reach, or widely distributed equipment and processes.
- Adaptability
  - The ability to adapt to new business requirements, customer needs, and changing conditions, or scale the deployment in response to business growth or customer requirements

CHALLENGES OF IOT

Sensors
- Limited resources
- Limited types of sensors

Scale
- millions of devices are connected to form IoT

Privacy
- which personal data to share with whom
- how to control

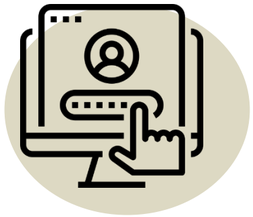
Security
- "things" becomes connected, so security becomes complex

Low Power Network
- Devices should remain connected to the Internet for years
- High network latency

Big data and Data analytics
- massive amount of sensor data
- different sources and various forms
- extract intelligence form the heaps of data

Interoperability
- various protocol, various architecture
- unavailability of standardized platform
- different technology leads to interoperability issue
- Recent IoT standards are minimizing this problem

SECURITY



Authentication – IoT devices connecting to the network create a trust relationship, based on validated identity through mechanisms such as: passwords, tokens, biometrics, RFID, X.509 digital certificate, shared secret, or endpoint MAC address.

Authorization – a trust relationship is established based on authentication and authorisation of a device that determines what information can be accessed and shared.

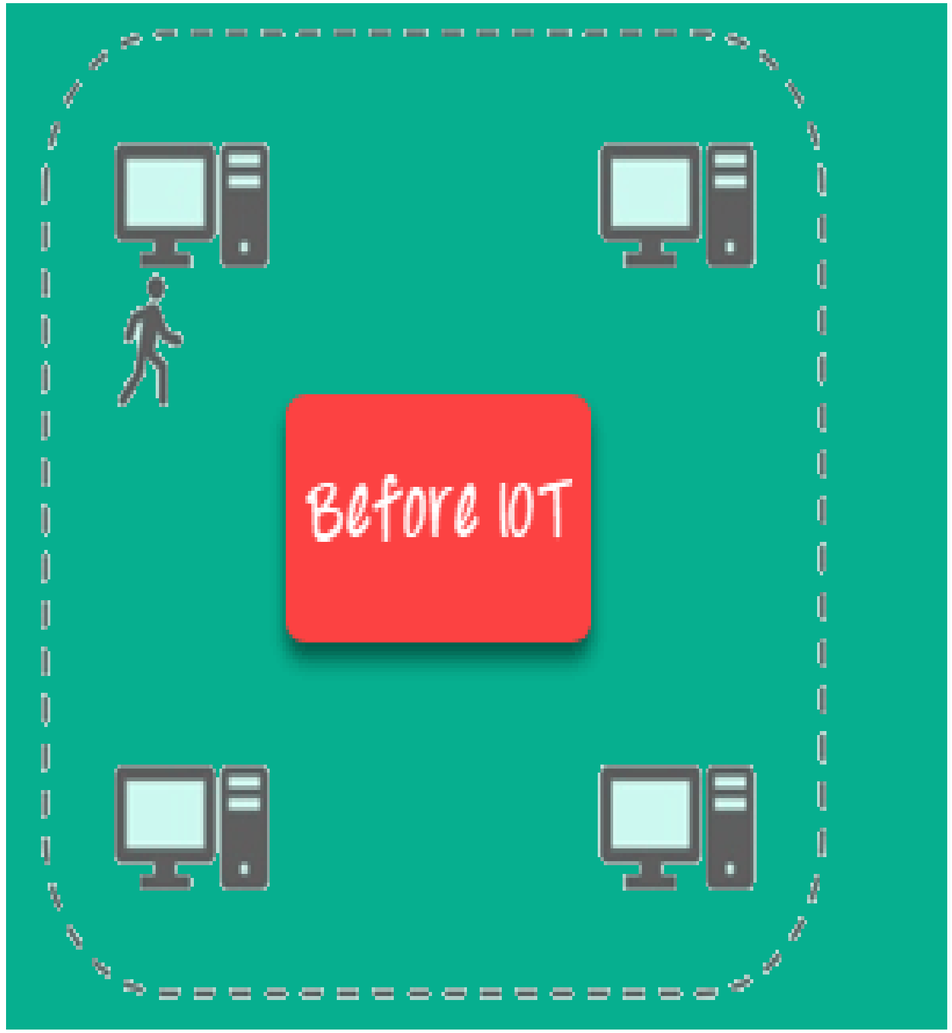
Network Enforced Policy – controls all elements that route and transport endpoint traffic securely over the network through established security protocols.

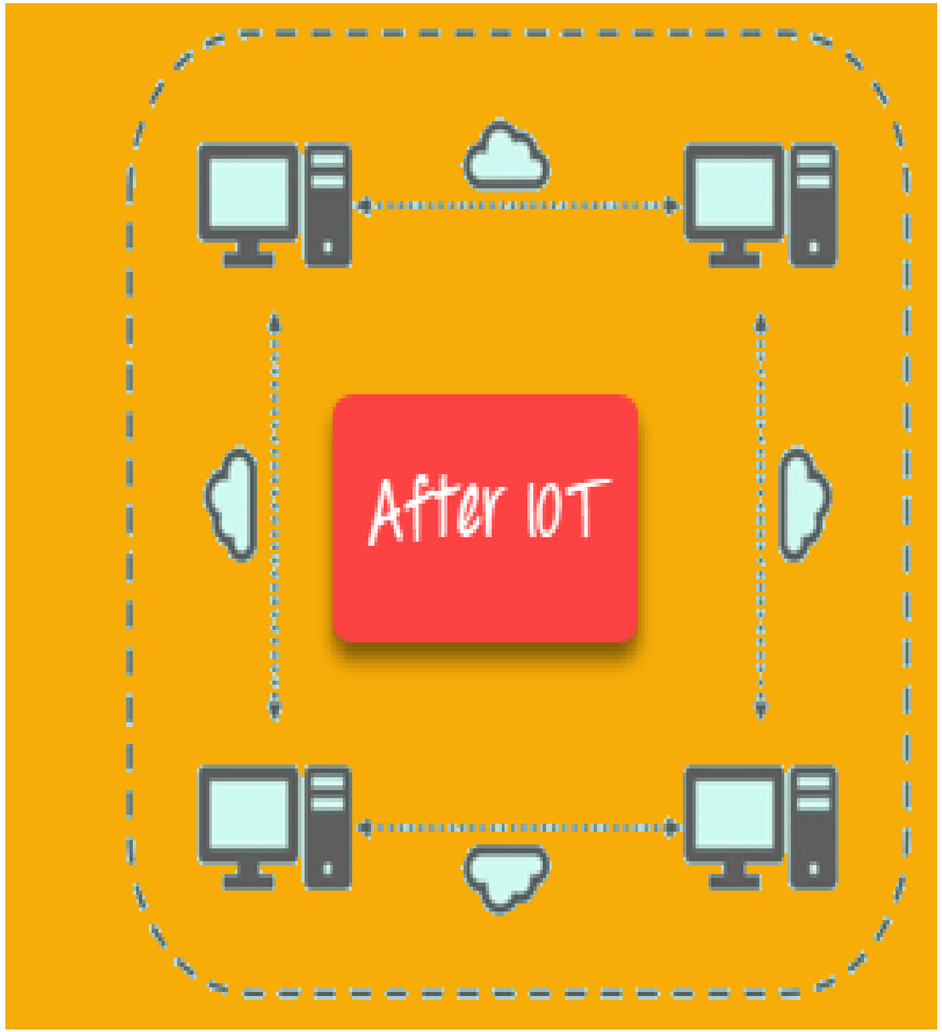
Secure Analytics: Visibility and Control – provides reconnaissance, threat detection, and threat mitigation for all elements that aggregate and correlate information.

MODERN APPLICATIONS

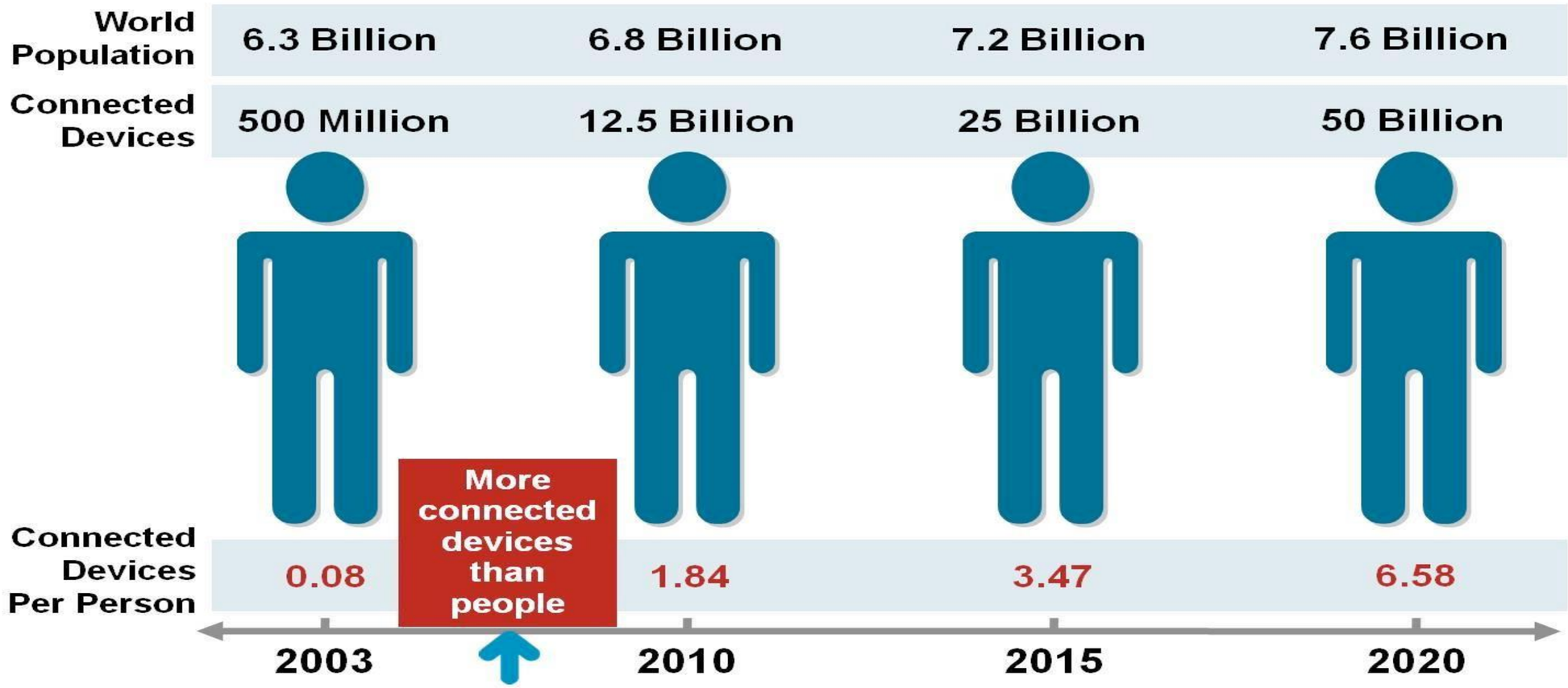
1. Smart Grids
2. Smart cities
3. Smart homes
4. Healthcare
5. Earthquake detection
6. Radiation detection/hazardous gas detection
7. Smartphone detection
8. Water flow monitoring

ADVANTAGES





CURRENT STATUS & FUTURE PROSPECT OF IOT



THANK YOU