Artificial Intelligence,Internet of Things & Smart Cities

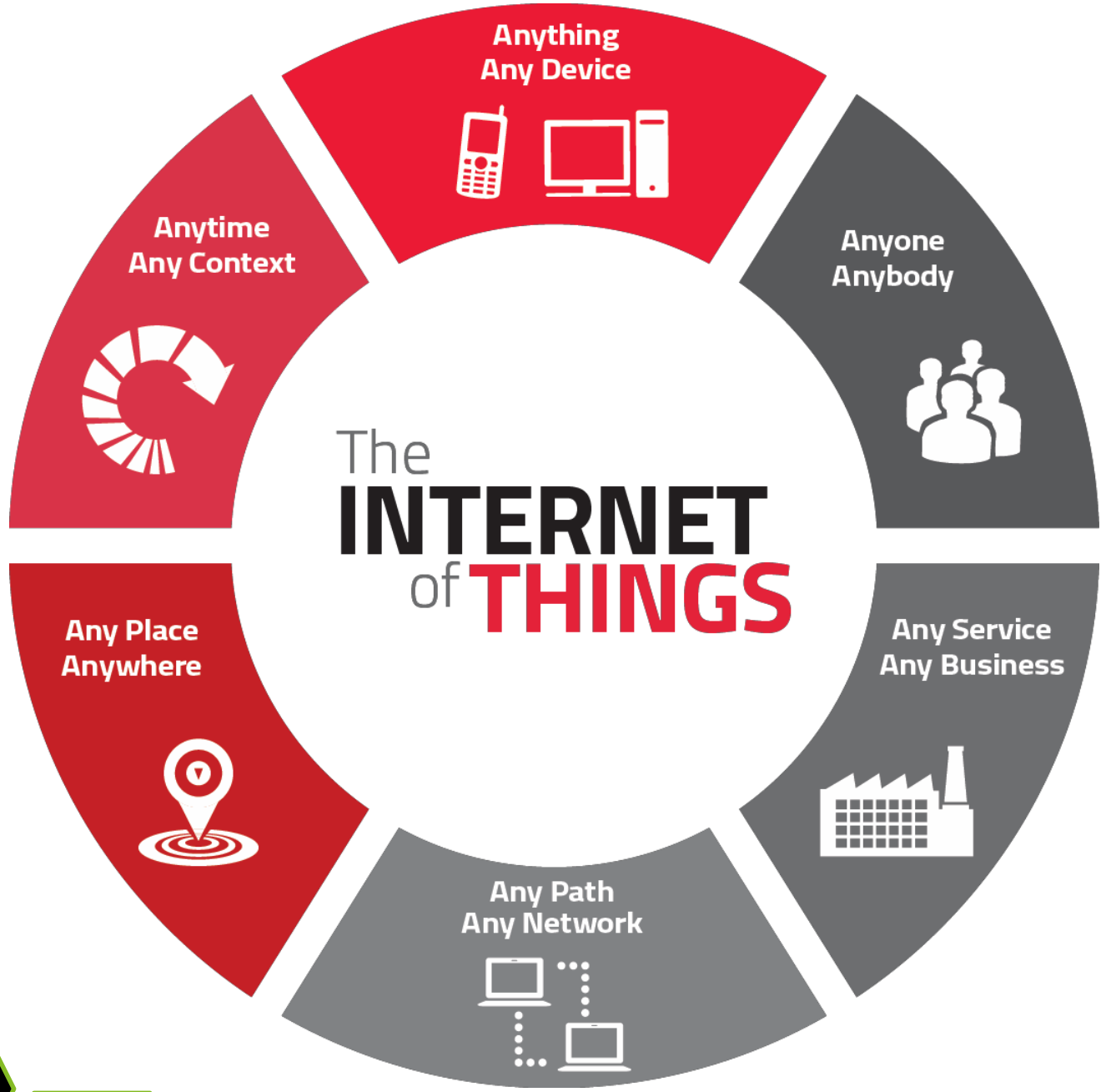
August 2023


The Internet is currently a human-to-human affair,
but that is CHANGING.
The Internet of Things is
EVERYTHING to EVERYTHING
communication.

1999!

"THE INTERNET OF THINGS IS ABOUT EMPOWERING COMPUTERS ...SO THEY CAN SEE, HEAR AND SMELL THE WORLD FOR THEMSELVES"

KEVIN ASHTON
INVENTOR OF THE TERM
"INTERNET OF THINGS"


Anything
Any Device
Anyone
Anybody
Any Service
Any Business
Any Path
Any Network
Any Place
Anywhere
Anytime
Any Context
The
INTERNET
of THINGS

What Is Internet of Things?

Internet of Things refers to intelligent, connected devices generating data for new services and providing actionable insights or triggers based on input stimuli

Definition: *The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items which are embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data*

25 Billion

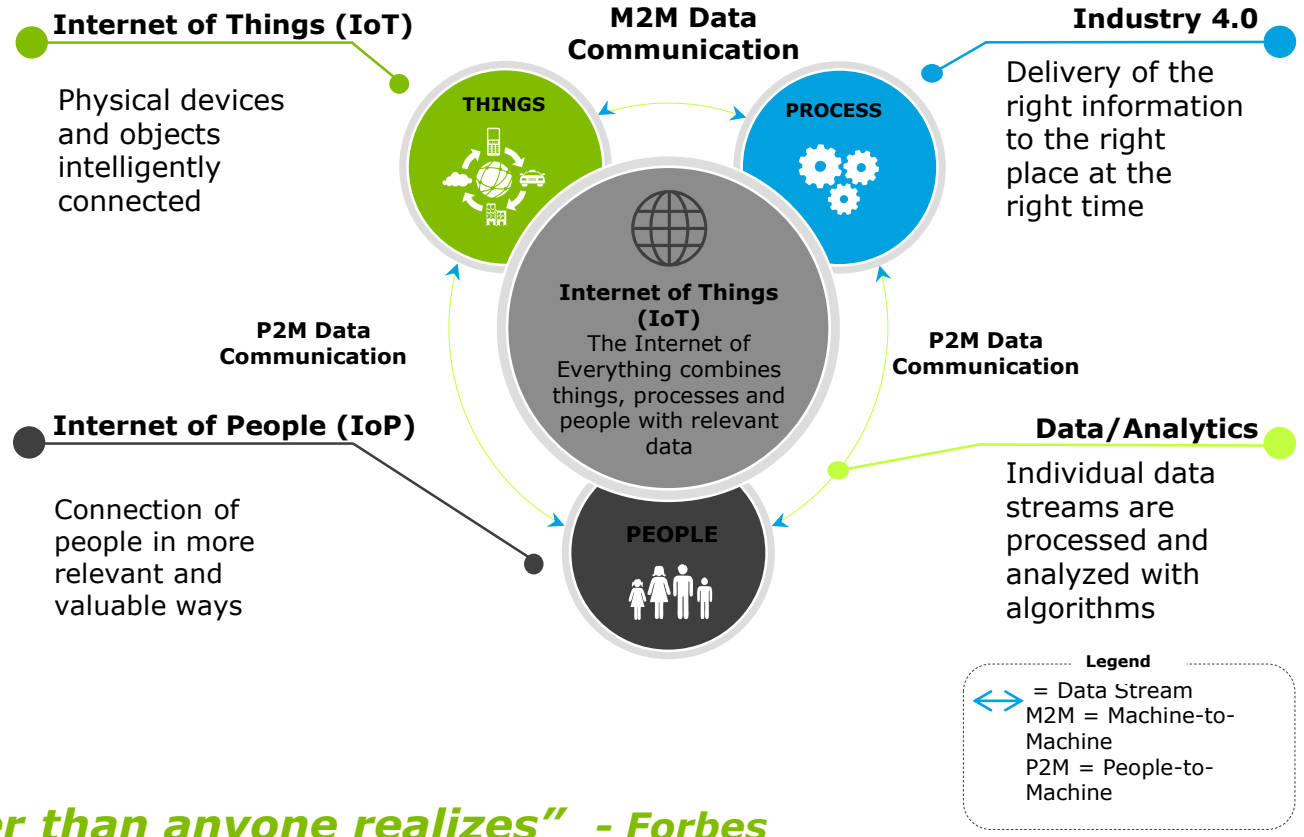
Installed IoT Devices[2] by 2020

$3.6 Trillion

Potential economic impact[1] per year by 2020

70% B2B

IoT value created in B2B use cases



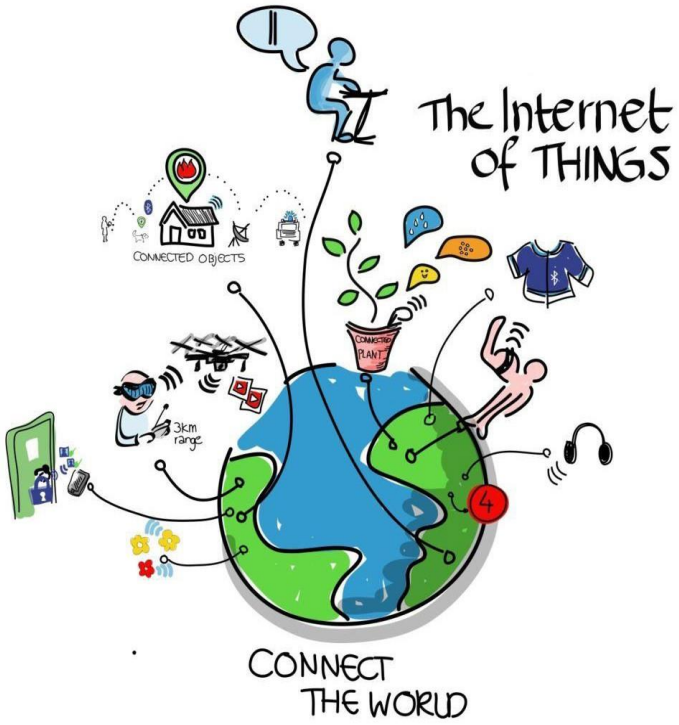
"The Internet Of Things is far bigger than anyone realizes" - Forbes

[1] McKinsey June 2015
[2] Gartner November 2014

Why IOT?

- Dynamic control of industry and daily life.
- Improves the resource utilization ratio.
- Integrating human society and physical systems.
- Flexible configuration.
- Acts as technology integrator.
- Universal inter-networking.

IOT Building Blocks



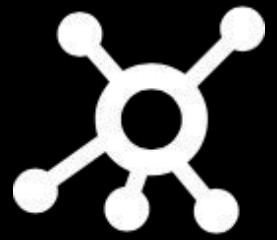
IOT Platforms And Enablement

TECHNOLOGIES THAT ENABLE IOT

Big data (unstructured data)

IPv6

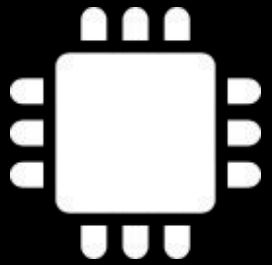
Cheap sensors (50% cheaper)



Cheap bandwidth

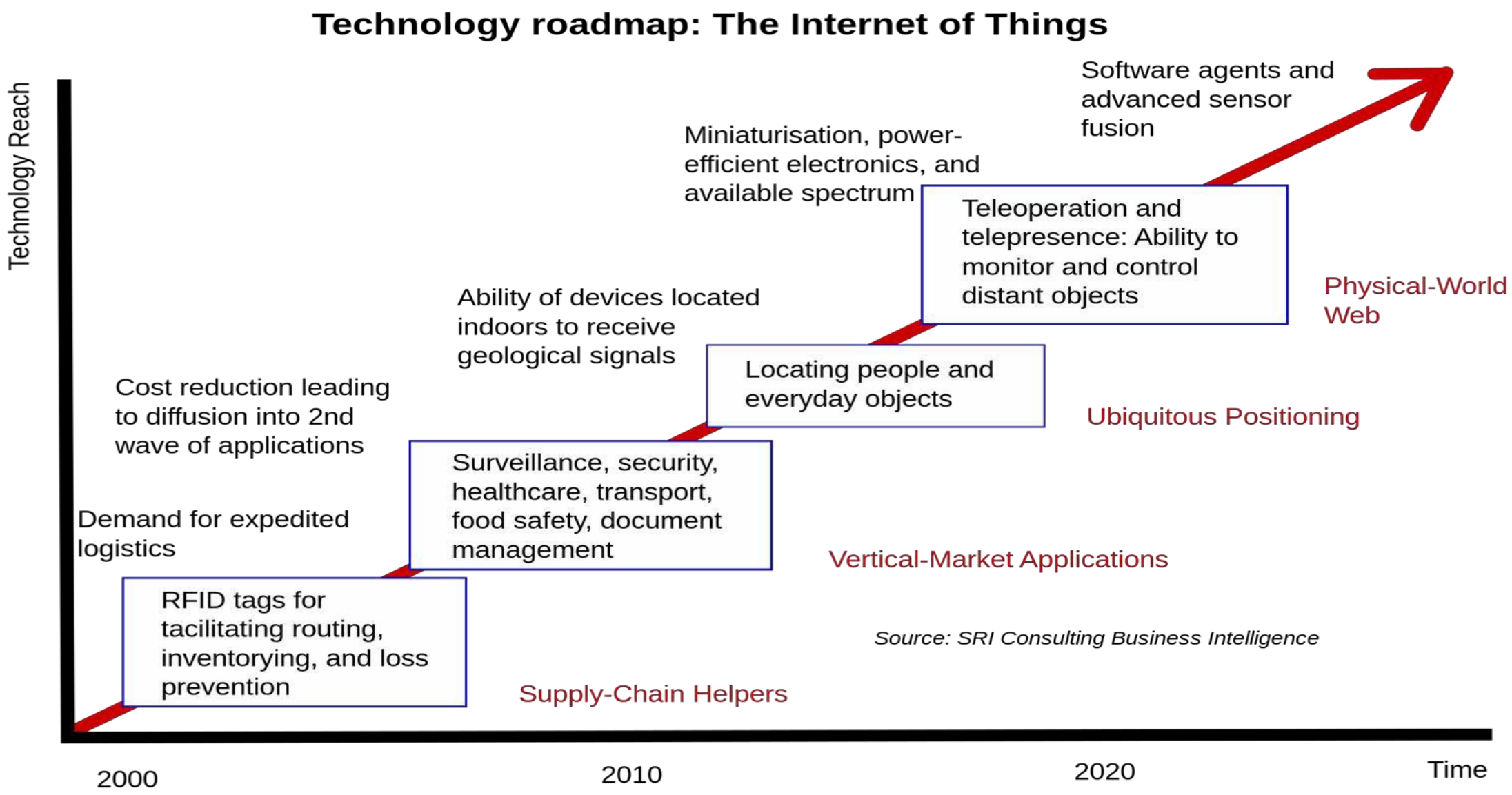
Ubiquitous wireless coverage

Smartphones

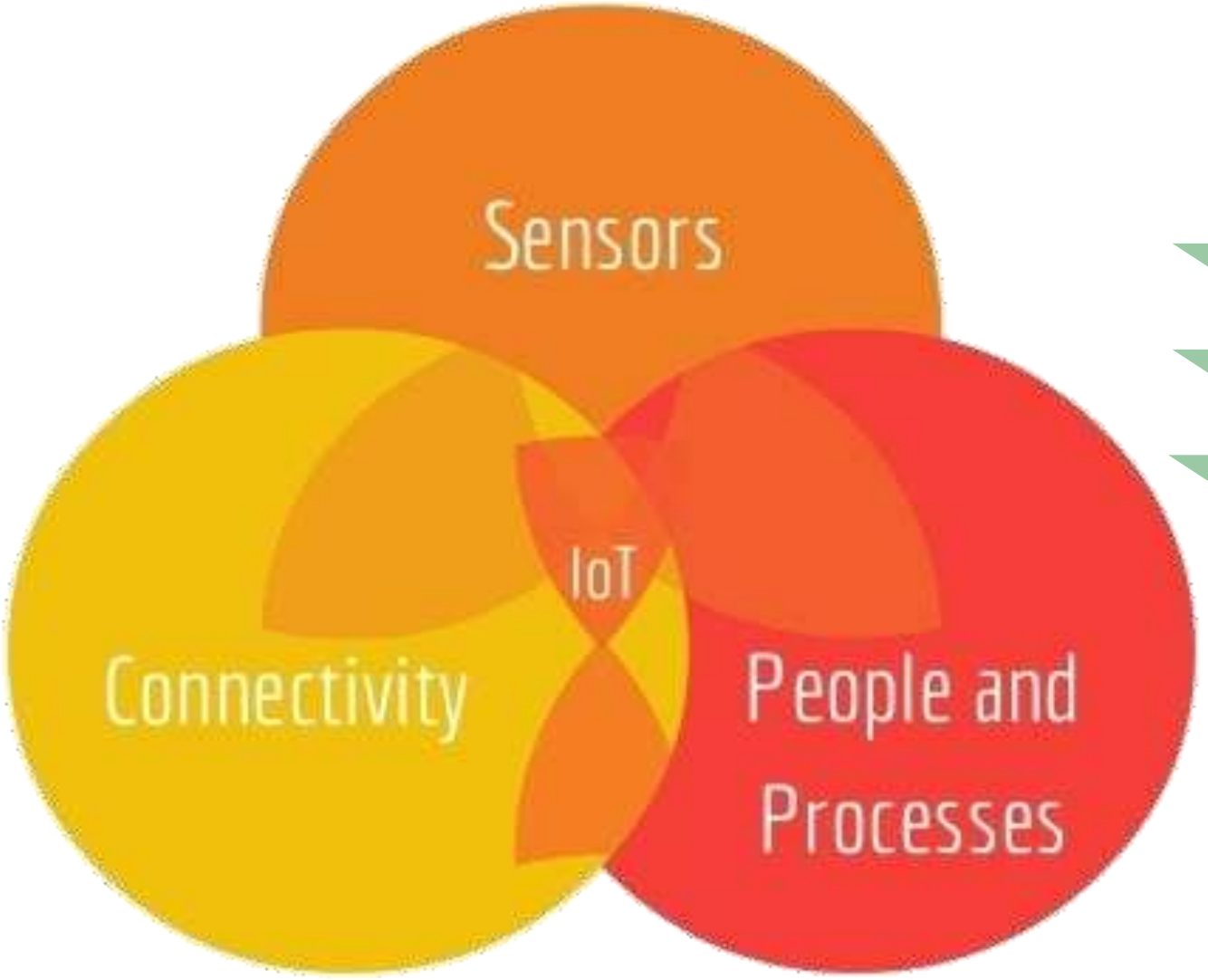


Cheap processing & smarter

IOT Technology Roadmap



IOT Components



Smart Systems and Internet of Things are driven by a combination of :

- Sensors
- Connectivity
- People & Processes

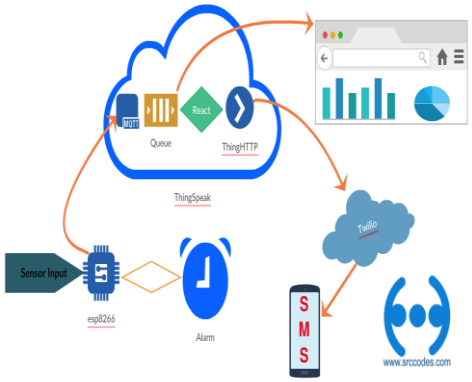
How Artificial Intelligence Internet of Things will impact the Industry

Smart Sense

Position/Presence/Proximity/machine vision/Optical/Ambient Light/Acceleration/Tilt/Electric/Magnetic/Leaks/Levels/Force/Load/Pressure/Flow/Chemical/Gas Acoustic/Sound/Humidity/Moisture/Temperature Motion/Velocity

AI enabled Connect

- WiFi
- Bluetooth
- Ethernet
- NFC
- RFID
- Powerline
- PAN
- LAN
- MAN
- WAN

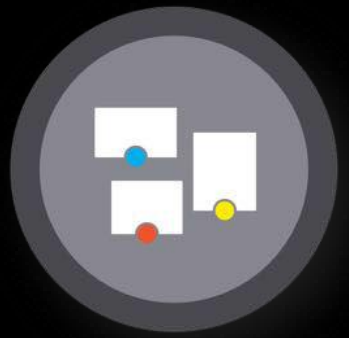


AI enabled React

Customer Relationship & Support
Analytics & Cloud API
Upgrades & Configurations
Remote monitoring & Maintenance
Controls & Automation
Supply chain Management
Security Energy
Mobile Device & Apps
Location & Tracking
Financial

4 STAGES OF IOT MATURITY

AI +Monitoring



AI + Control

AI +Optimization.

AI +Autonomous

Applications of Internet of Things

Manufacturing

- Predictive Maintenance
- Supply Chain Optimization
- Asset Tracking
- Automate Workflows
- Personnel Safety

Energy & Resources

- Smart Grid
- Leagage Prevention
- Wellhead optimization
- Asset Optimization
- Personnel Safety

Retail / Consumer Products

- Consumer Marketing
- Reimagined Store Front
- Intelligent Replenishment
- Supply Chain Management
- Memorable Experiences

Life Sciences / Healthcare

- Clinical Trials
- Patient Experience
- Equipment Tracking & Diagnostics
- Remote Monitoring
- Inventory Management

Auto / Transportation

- Dealership of the future
- Remote diagnostics
- Fleet management
- Autonomous vehicle

Military

- Connected battlefield
- Supply chain
- Fleet Tracking

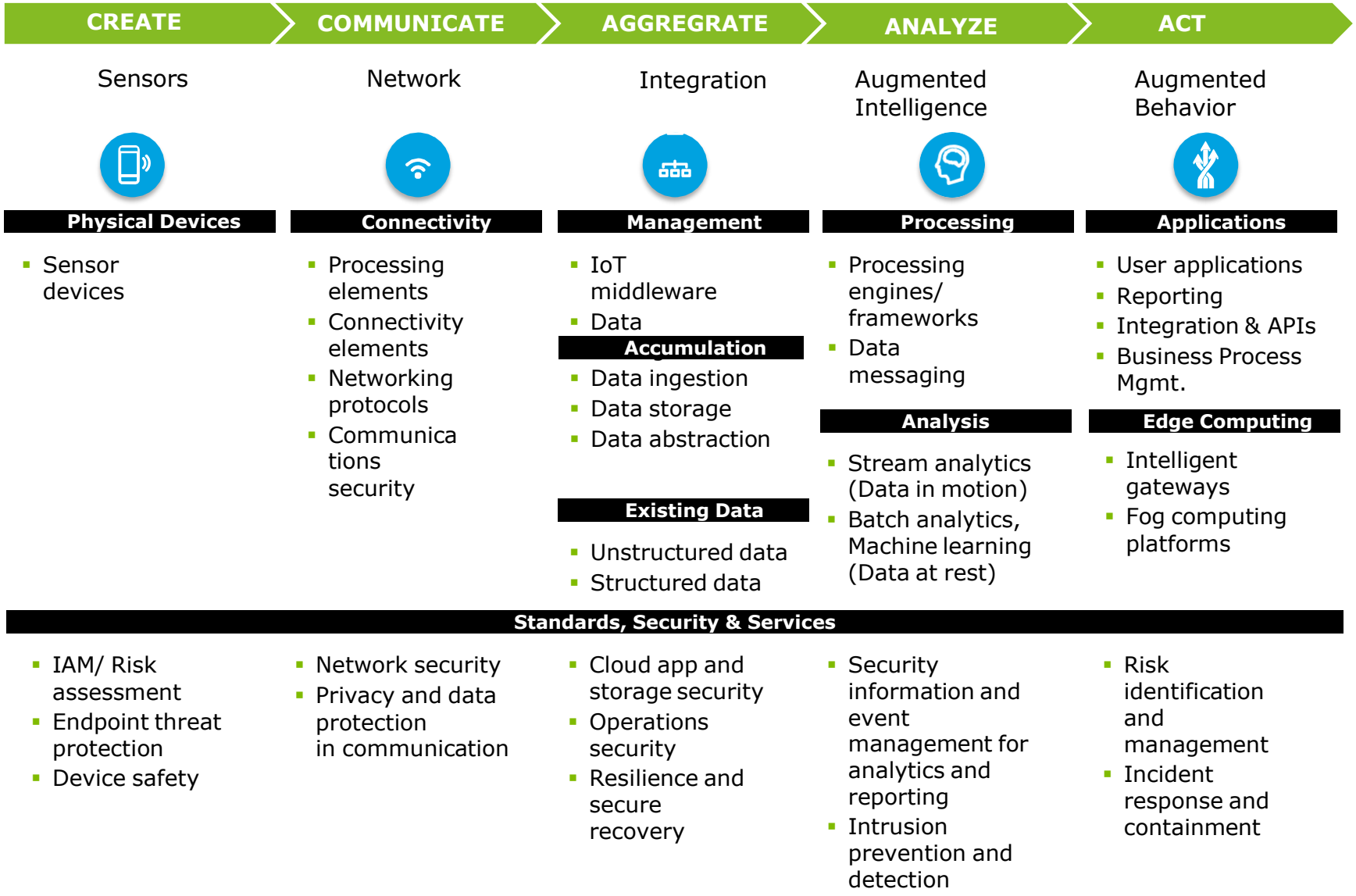
Financial Services

- Perf-based Insurance – Auto, health and home
- Personalized risk profiles
- Retail banking

Smart Cities

- Smart lighting
- Transportation/ Energy Management
- Smart parking
- Smart waste

Evolution of Internet of Things



Cyber Security –IOT Implications

SECURITY CONCERNS:

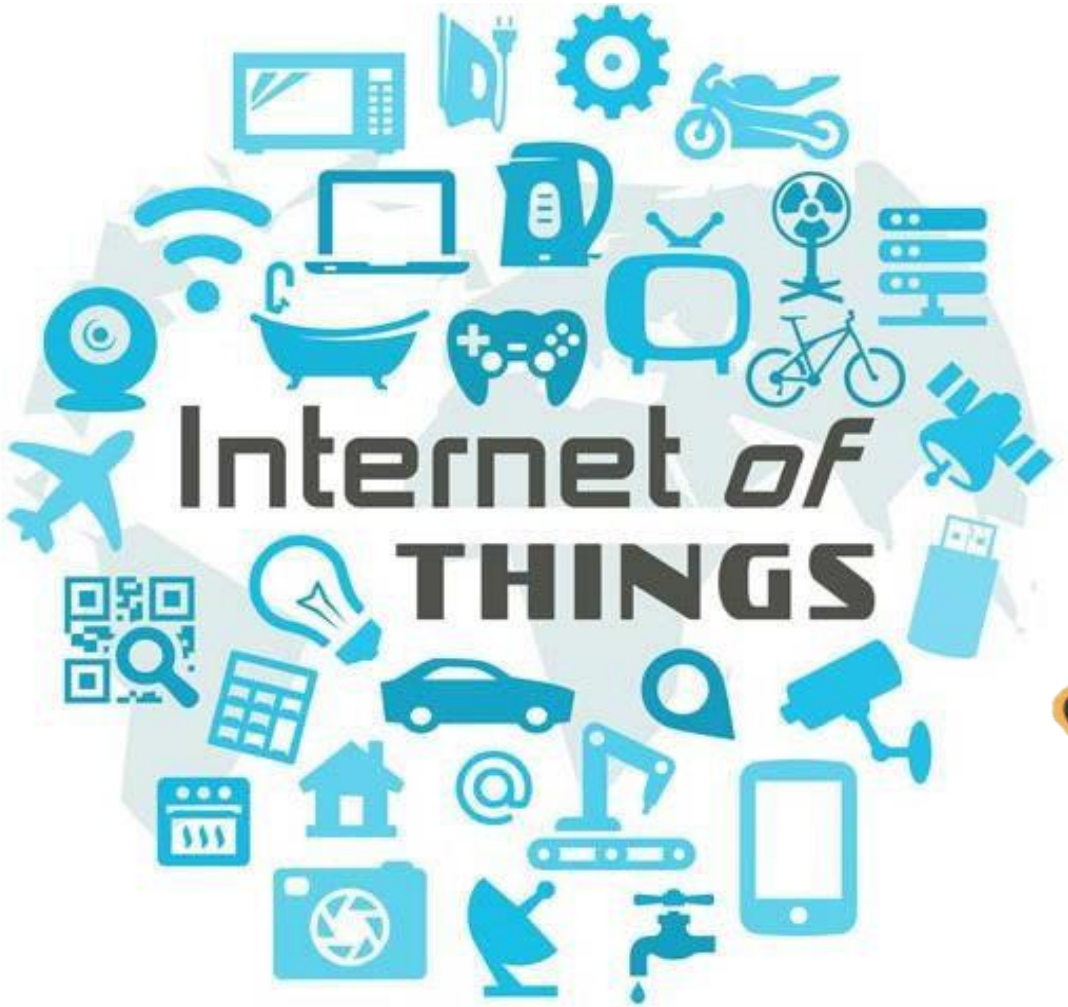
- Pretty much anything will have an IP address that can be used to communicate with it.
- Networks with increase of traffic
- Data storage
- Security
- Applications

MASSIVE ATTACK SURFACE:

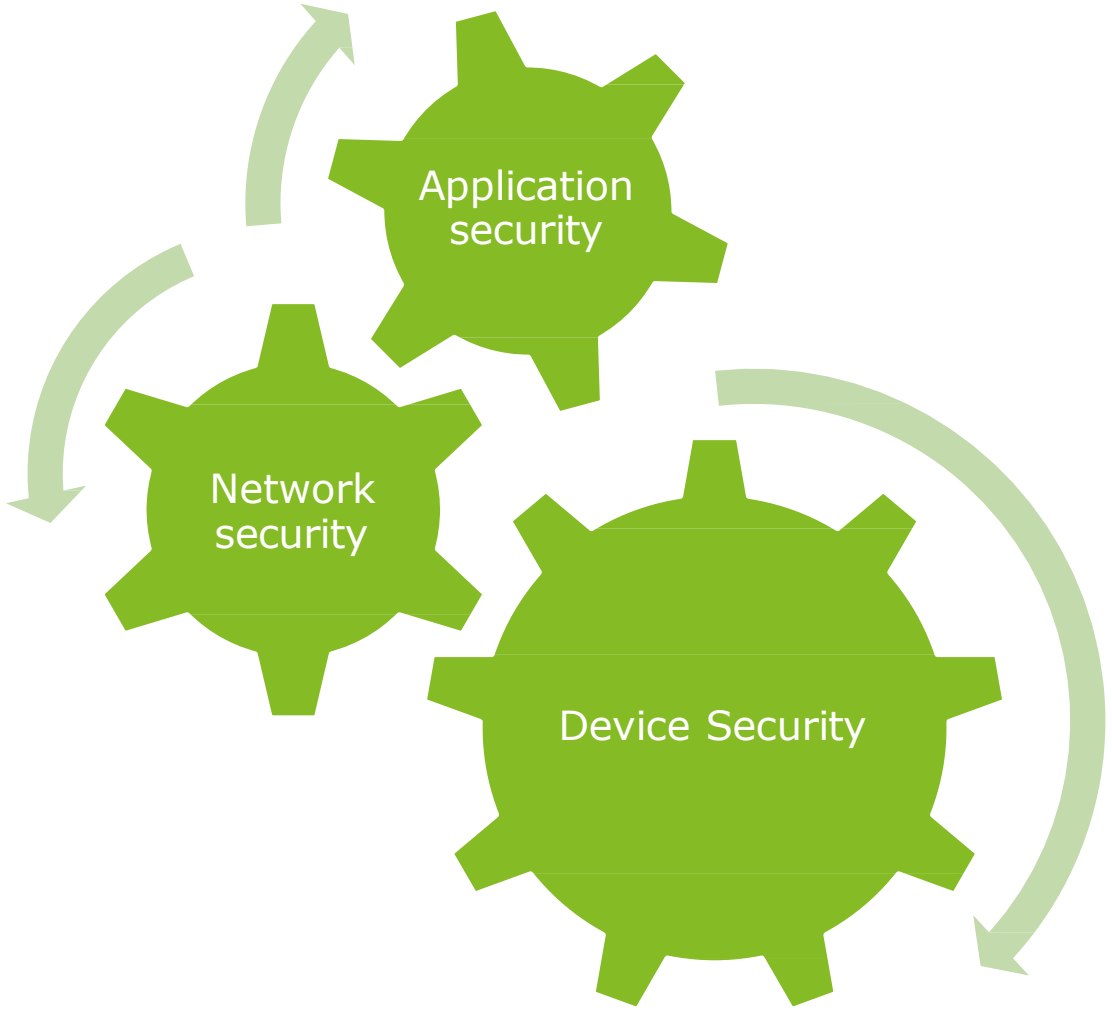
- Lots of data to analyse
- Lots to protect
- Lots to hack
- Botnet opportunity.

WELL KNOWN IT HACKS:

- Mirai Botnet
- Jeep Hack
- St Jude's Cardiac devices
- Fish tank in Casino hack



IOT Security – Where To Start



Smart City Concept

“If the cities of the past were shaped by people, the cities of the future are likely to be shaped by ideas, and there are a lot of competing ones”

Introduction to Smart cities

A smart city is an urbanized area where multiple sectors cooperate to achieve sustainable outcomes through analysis of contextual real-time information shared among sector-specific information and operational technology systems.

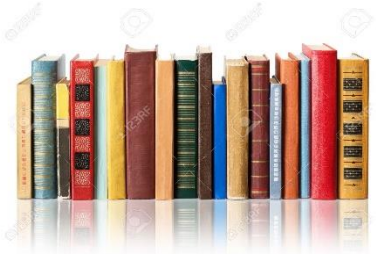
Reasons why we focus on Smart cities

More than half the world lives in cities

More than 60% of cities have yet to be built

Cities are at the forefront of global innovation

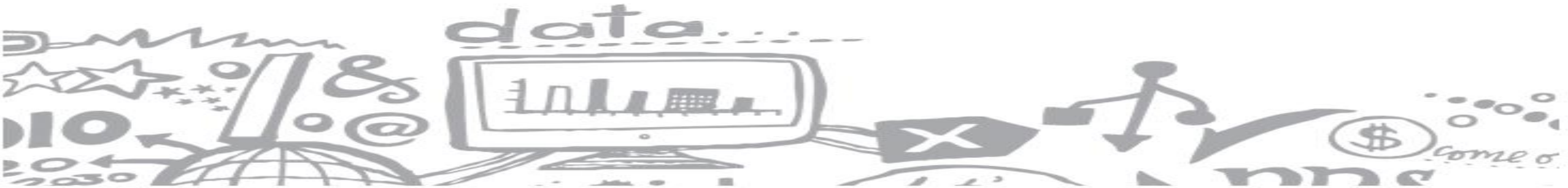
By 2050, 70% of World’s population will live in cities



Cities have been center of civilization, Life and Knowledge for centuries

Final Aim of Smart cities

1. To Support better living, create more opportunities, support stronger and more cohesive communities and improve the quality of life overall for all residents
2. To make a better use of Public resources
3. Reducing the operational costs of the public administrations



IoT in Smart cities

01 Structural Health of Buildings

02 Waste Management

03 Air Quality

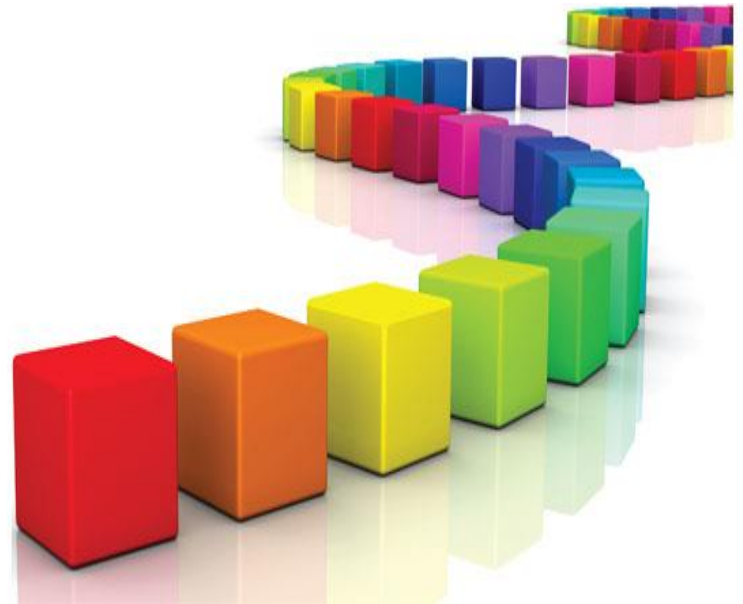
04 Noise Monitoring

05 Traffic Congestion

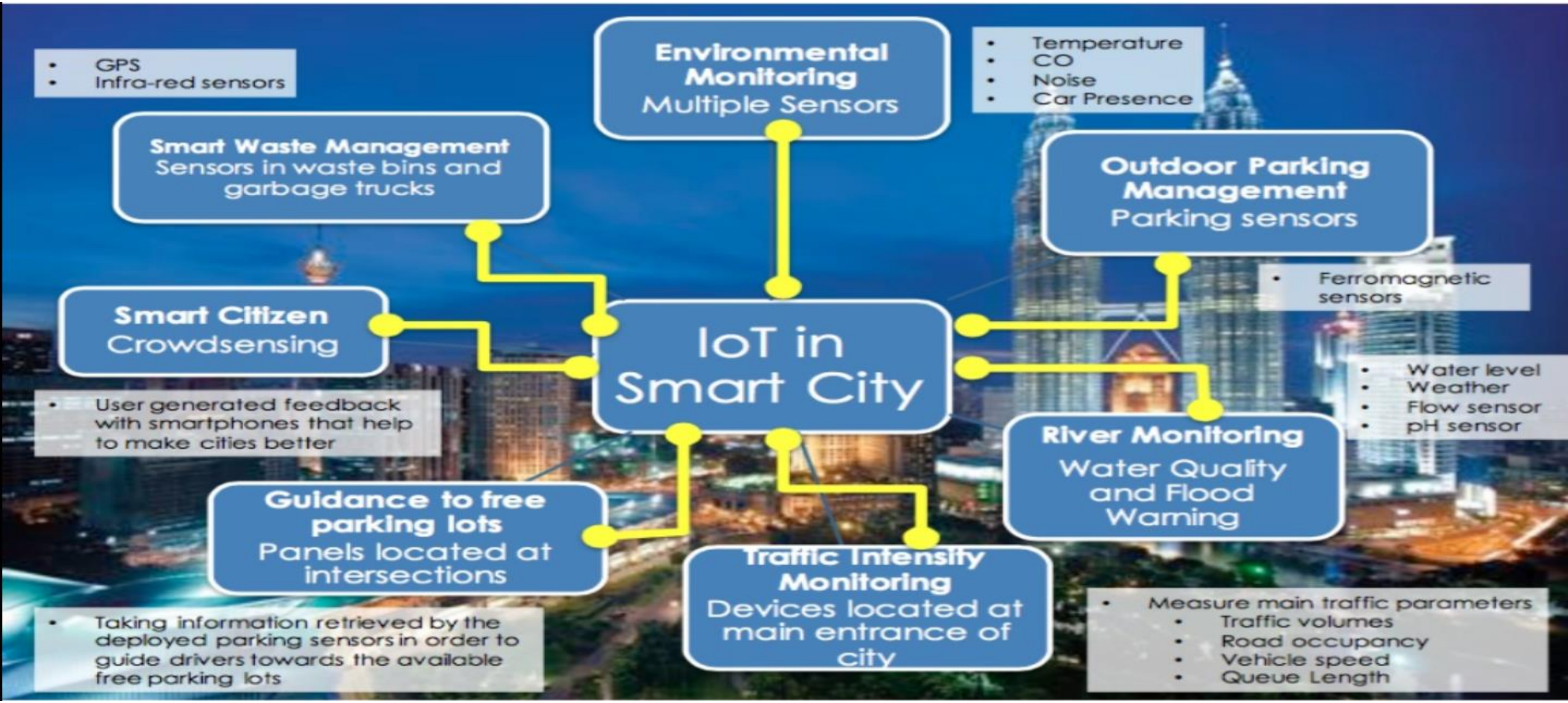
06 City Energy Consumption

07 Smart Parking

08 Smart Lighting



Artificial Intelligence + IoT in Smart cities



Key Parameters of a Smart City

AI powered Smart Energy	•Digital Management of Energy; Smart grids, Smart meters, Intelligent energy storage
Smart Buildings	•Intelligent mobility; Advanced traffic management system (ATMS), Parking management, ITS-enabled transportation pricing system
Smart Mobility	•Intelligent mobility; Advanced traffic management system (ATMS), Parking management, ITS-enabled transportation pricing system
Smart Technology	• Seamless Connectivity; 5G connectivity, Super broadband, Free Wi-Fi
Smart Infrastructure	• Digital Management of Infrastructure; Sensor networks, Digital water and waste management
Smart Governance & Smart Education	• Government-on-the-Go; e-Government, e-Education, Disaster management solutions
Smart Healthcare	• Intelligent Healthcare; Technology, Use of e-Health and m-Health systems Intelligent and connected medical devices
Smart Security	• Intelligent Threat Detection; Surveillance, Biometrics, Simulation modelling and crime protection, Advanced proactive antivirus protection

How IoT will play a role Smart cities

Fundamental to the creation of smart cities is the generating, analyzing and sharing of large quantities of data. Indeed the main aim of smart cities technologies is to make cities data-driven; allowing city systems and services to be responsive and act upon data in real-time.

Intelligence: the first and most important stage of security is surveillance and intelligence gathering. This calls for equipment such as CCTVs and Biometrics hardware and software to collect the essentials in its raw, unprocessed form. Secured network for transmission of data is important to ensure non- tempering of data.

Analyzing Data collected: Analytics help digest, decode and make sense of the terabytes of information and data collected, by providing secured storage, analysis and forensic tools. Change from byte-sized to bite-sized for effective prevention against threats or reaction to a calamity and provide situational awareness.

Mobilizing the Resources: There is human intervention in any security installation with physical security apparatus from perimeter protection to communication devices for personnel on the move. The effective mobilization of people and equipment is crucial to the entire infrastructure of a steadfast and secured location.

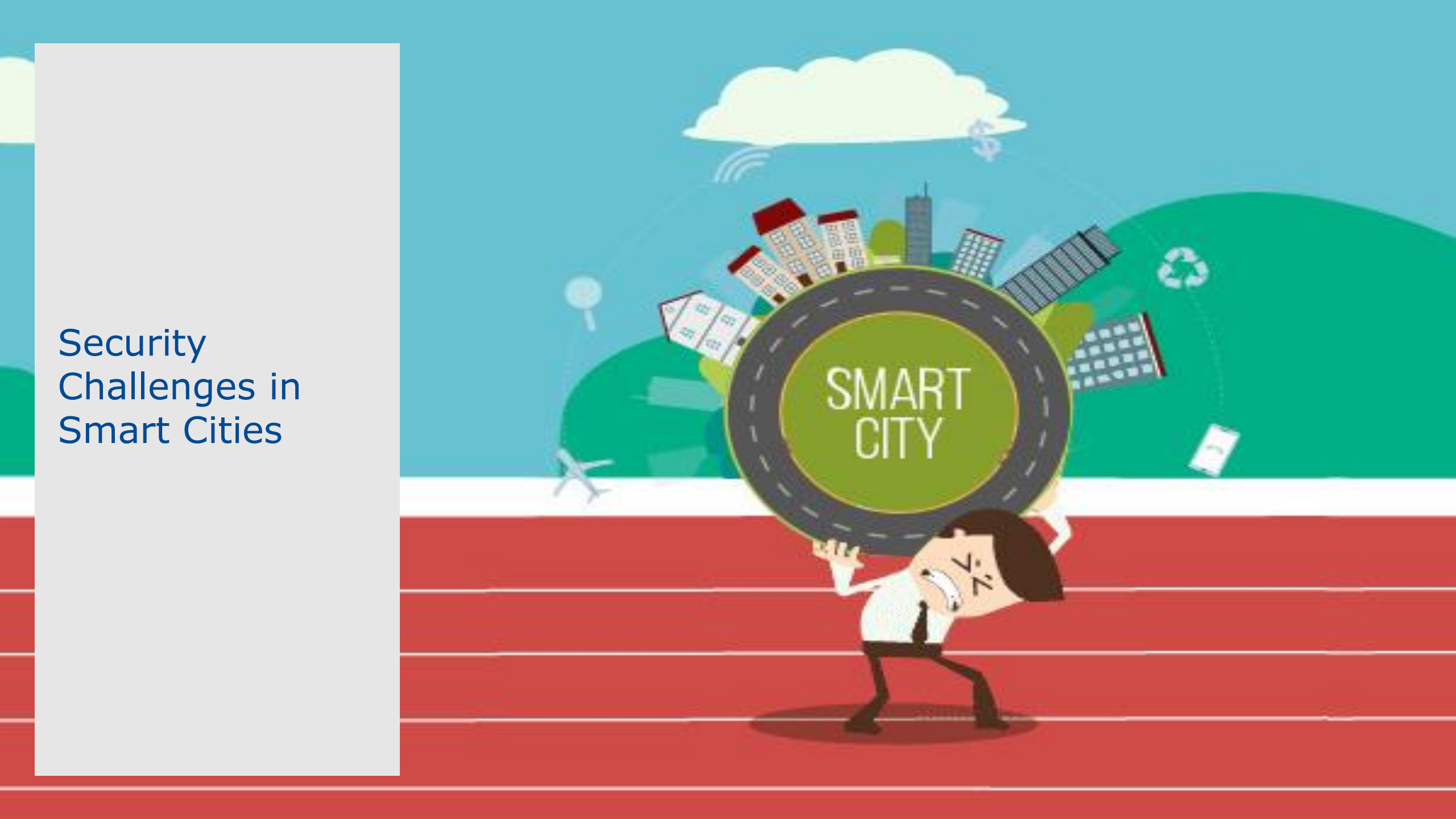
Future of Smart Cities

The global smart city market is expected to reach US$1.565 trillion in 2020, with one-half of smart cities from North America and Europe*. E-Services to citizens, such as e-Payments, e-Exchange, e-Sharing, etc., will empower citizens with real-time access to personal data and related services.

The multiplying effect of today's cybersecurity challenges presents an opaque universe of threats that often come from unexpected or unforeseen domains which have an escalating effect.

- The speed of change – can the Smart City's cybersecurity keep pace?
- New product launches, mergers, acquisitions, market expansion, new technology
- A network of networks has made data accessible everywhere, any time
- One vulnerable device can lead to other vulnerable devices
- Traditionally closed operating systems can be accessed externally
- Cloud vulnerabilities and Big data – storage and server security issues
- Bandwidth consumption from billions of devices will put a strain on the spectrum of other wireless
- communications.

Security Challenges in Smart Cities



Security Challenges in Smart Cities

1 | Data Privacy and protection concerns

Smart city technologies capture data relating to all forms of privacy and drastically expand the volume, range and granularity of the data being generated about people and places. Privacy can be threatened and breached by a number of practices which are normally treated as unacceptable, however are part of operations in a smart city eco system.

- Surveillance: Watching, tracking, listening to or recording a person's activities
- Aggregation: Combination of various aspects of data about a person to identify a trend or pattern of activities.
- Data leakage: lack of data protection policies can lead to leakage or improper access of sensitive information
- Extended usage: use of data collected for period longer than stated or for purposes other than the stated purpose without the subject's consent

2 | Insecure Hardware

One of the major concerns about smart cities sensors in the equipment; buildings etc. are insecure and not tested thoroughly. Owing to lack of standardization of IoT devices, the sensors are prone to hacking. Notorious individuals can hack the sensors and feed fake data, causing signal failures, system shutdowns etc.

3 | Larger Attack Surface

Smart city operations utilize complex, networked assembly of ICT infrastructure to manage various services. Any device that is connected to the network is vulnerable to being hacked; the number of potential entry points is multiplied in Smart Cities. By compromising a single device, it is possible to attack the entire system or network.

4 | Bandwidth Consumption

Thousands of sensors, or actuators, trying to communicate to a single server will create a flood of data traffic which can bring down the server. Additionally, most of the sensors use an unencrypted link to communicate, and hence, there are possibilities of security lapses. The bandwidth consumption from billions of devices will put a strain on the spectrum of other wireless communications, which also operate on the megahertz frequencies like radio, television, emergency services, etc.

5 | Application risk

Apps have accelerated the integration of mobile devices within our daily lives. From mapping apps, to social networking, to productivity tools, to games, apps have largely driven the smartphone revolution and have made it as significant and as far- reaching as it is today. While apps demonstrate utility that is seemingly bound only by developer imagination, it also increases the risk of supporting Bring Your Own device (BYOD) in a corporate environment.

As the organization enables employees to bring their own devices, the need for using the same devices to access work-related data inevitably presents itself. This presents mainly two security risks:

- Malicious Apps(Malware)
- App Vulnerabilities

6 | Simple Bug with Huge impact

A simple software bug can have huge impact. As Smart Cities will run on hundreds of systems and devices managing critical services, a simple software bug can have huge impact. For instance November 2013 Bay Area Rapid Transit

Getting ahead of Cyber crimes

Early warning and detection of breaches are decisive to being in a state of readiness, meaning that the emphasis of cybersecurity has changed to threat intelligence. A state of readiness to deal with cyber attacks requires behaviors that are thoughtful, considered and collaborative. No organization or government can ever predict or prevent all (or even most) attacks; but they can reduce their attractiveness as a target, increase their resilience and limit damage from any given attack.

A state of readiness includes:

Components of a Safe smart city

Surveillance system and equipment:

The aim of smart city is to provide shared security presence and real time surveillance with the use of video cameras. The cameras collect data in image or video format which may be monitored from a central location, and allow first responders to act instantly in an emergency situation.

AI Enabled Video Analytics:

Video analytics is the capability of automatically analyzing videos to detect certain objects, behavior, spatial and temporal events. This is used in a wide range of domains, including entertainment, Health care, surveillance, home automation etc. These Video analytics tools can be used with a wide range of modules for various purposes and can work as a proactive monitoring tool, triggering alarms to signal immediate attention of concerned teams.

Data Center:

The data center is the centralized storage space for all the data collected from the multiple sensors in the network. The data center provides real time data to monitoring centers for effective operations. The data center hosts applications for the operation of video management, analytics and traffic control etc. The design of data center depends on the kind of applications that are run in the smart city.

Command Center:

The command center provides an infrastructure that can assess the integrated information provided by the data center such as live video for incident response. It aids in quicker analysis of data for better decision making.

Securing Smart Cities

Possible Solutions to Challenges

Build a risk- based approach to cyber security

- Develop a clear structure for risk assessment and management
- Use threat modeling to assess threats.
- Document and review risk acceptance and exceptions.
- Make risk assessment and management an ongoing process.

Set clear priorities

- Educate city leaders to understand and support the principles and to manage priorities.
- Consider resilience.
- Leverage procurement processes to reflect priorities and risks.

Define minimum ICT security baseline

- Establish minimum security baselines.
- Define clear responsibilities for supporting a security baseline.
- Establish a system for continuous security monitoring.

Possible Solutions to Challenges

Share and coordinate threat and vulnerability information	• Set expectations for sharing threat and vulnerability information. • Create a cross-city mechanism for sharing. • Run cyberdrills to test game plans. • Emphasize privacy and civil liberty protections in threat information sharing. • Apply relevant national or international standards for information sharing.
Build incident response capabilities	• Create a Computer Emergency Response Team (CERT). • Create clear ownership. • Engage private sector and national resources. • Enable consistent incident classification. • Test incident response capabilities and processes.
Boost public awareness, education, and workforce training	• Develop public awareness campaigns. • Cultivate employee development and workforce training programs.

Q&A