Unit-2 Chapter:1 Lecture notes (Topic: IoT architecture and security challenges)

The term Internet of Things (IOT), also known as Internet of Objects refers to the networked interconnection of everyday objects, which is generally viewed as a self-configuring wireless network of sensors whose purpose would be to interconnect all things.

Today the world is totally dependent on the information provided on internet, which is captured by taking images or through text. This clearly specifies the major involvement of a human being for collection of the information. But the problem with human involvement is that, people have limited time and less accuracy, which leads to inappropriate and inconsistent data. Hence, such a system is needed which can automatically capture the data and transfer it to the internet without any human to machine interaction. Internet of things is a scenario in which all the things are connected to the internet through the information sensing devices for the purpose of intelligent identification and management. These things are provided with the unique identifiers which can be read using RFID tags with the help of sensors (information sensing devices). The thing in the internet of thing 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 the pressure is low or any other manmade object that has a unique IP address

with the ability to be connected to the network for the transfer of the data . There is a major participation of wireless technology, Micro-electromechanical Systems (MEMS) and the internet in the making of IOT [2]. One of the basic things needed to sense the object in the environment is RFID. Sensing can be possible by assigning each object a unique identifier and then connected to the internet, for smart processing by the transfer of information. IPv6 is playing a very important role in the development of IOT, by using its huge address space one can easily assign an IP address to every thing on this planet and could transfer the data over network.

IOT is one of the upcoming concepts of technological innovation in the field of networks which will help not only in the industrial development but also in the day to day life of a human being, hence now days IOT is being the research emphasis topic for the researchers and for the enterprises. The typical scenario of IOT is shown in figure 1, depicting the interconnection among things like smart television, phones/laptops, smart refrigerator and smart individual etc.

via internet. One can say that by the smart use of IOT, it would be possible to know when the things need to repair, recall or replace without any human interference; which greatly reduce the waste and loss of the objects. The main objective of this paper is to provide the understanding of security issues of IOT which needs to be studied along with their countermeasures. This paper presents a brief idea of IOT which includes the architecture of IOT, security issues at each layer and countermeasures. These issues would be studying theoretically using parameters like authenticity, integrity, availability, confidentiality etc. The remainder of this paper is organized as follows. In this the architecture of IOT have presented. It gives main emphasis on security parameters and issues faced by IOT with its countermeasures. Finally, concluded the paper along with the direction for further work.

2. ARCHITECTURE OF IOT

Internet of things is composed of two words i.e. “Internet” which give a look of interconnected networks and “Things” which clearly shows some objects. But when these two words put together gives a means of “a world-wide network of interconnected objects, uniquely addressable, based on standard communication protocols” Internet of things does not have a unique definition but as per the different definitions by several research groups around the world, a common concept can be drawn as, when objects can sense and communicate, the intelligent decision making and management is possible without human to machine interaction. Below it present the architecture and security of IOT. Real time working of IOT is possible through the integration of various technologies together. Xiong Li, Zhou Xuan in described the general architecture of trusted security system based on IOT. Security system such as trusted perception module, trusted terminal module and trusted network module. In this paper, a layered architecture of IOT is presented that gives an idea about basic architecture of IOT. Generally, IOT is divided into three layers: Perception layer, Network layer, and Application layer . All of these three layers have large scale of information with different enabling technologies and features as shown in below Perception layer: The main working of IOT i.e. collection of information is done at the perception layer with the help of different devices like smart card, RFID tag, reader and sensor networks, etc. It has a feature of comprehensive sensing through the RFID system to get object‟s information anytime and anywhere. Each RFID electronic tag has a unique ID called Electronic Product Code (EPC) which is the only searchable ID allocated for

each physical target. Extra information about the product is given by a string of figures imposed on it such as manufacturer and product category with its manufacturing date and expiry date etc.

Network layer: The data gathered by sensors used to be sent to the internet via network layer with the help of computers, wireless/ wired network and other components. Hence network layer is mainly responsible for the transmission of information with the feature of reliable delivery hence this layer also includes the functionality of transport layer. Application layer: Analyzing the received information and making the control decisions to achieve its feature of intelligent processing by connection, identification and control between objects and devices. Intelligence means makes use of intelligent computing technology such as cloud computing and process the information for intelligent control like what to do and when to do things hence this layer is also called as process layer. In the next section a brief idea of security issues at each layer has given.

3. SECURITY OF IOT

Various security issues of IOT has been about Security of Things such as Perceiving Security for Information Collection, Transmission Security for Reliable Data Transfer, Processing and Application Security for secure information handling. Below these issues have covered in detail. 3.1 Security Issues The growing use of IOT system needs a powerful protection against all possible attacks or vulnerability. Hence security is needed at each layer of the IOT system; each layer either consists of devices, applications or networks. Some classified security issues at each layer are as given below:

3.1.1 Security at Perception Layer

Perception layer mainly includes: Smart card, Reader, RFID tag, Sensor network. Each of these devices has following vulnerability which leads to be a security issue of IOT such as sensor attacks, sensor abnormalities, radio interference .

3.1.1.1 Terminal security issues

For perception of things it needs a large number of terminals, terminals are used for real-time data collection to be presented to the user. This process needs an authentication and data integrity. Due to the wireless nature of communication, IOT can face threat from the hackers, virus attacks etc. The main problems existed in perception terminals include leakage of confidential information, tampering, terminal virus, copying and other issues.

3.1.1.2 Sensor network security issues

The sensor nodes are responsible for data transmission, data acquisition, integration and collaboration. As they operate on their own battery with less security protection, they can face complex security issues as follows:

- Invoking Malicious Codes: Malicious programs such as worm which does not require any parasitic file, can easily affect the wireless and sensor network, hence it will be very difficult to detect the malicious code and act accordingly.
- Defect of the tag: Due to the limited cost of tag, it is not possible to provide enough security which leads to illegal use of legal reader due to which an attacker can easily get the information on tag and can illegally access RFID system without any authorization by counterfeiting. Any rewritable tag can be copied, decoded or fabricated by the attacker.

3.1.2 Security at Network layer

Network layer mainly including Computers, Wireless or wired network, faces security issues such as network content security, hacker intrusion, illegal authorization .

3.1.2.1 Data transmission security issue

The goal of network layer is to transmit information, the information need to be transmitted securely. The security of the network layer is of two main types: The first is from the security risks of the IOT itself; the second is from the related technologies and protocol defects during design and implementation . In wireless networks, nodes can move freely, they can join or leave the network at any time without any prior authentication. This makes wireless networks to be more malicious or vulnerable for the security concern. IOT network should have that capacity to handle such malicious destruction, but as per the researchers existing mechanism is not enough to handle this security issue.

3.1.3 Security at Application layer

Application layer mainly includes the intelligent devices for effective decision making. Each of these has some vulnerability which leads to be an issue of the security of IOT.

3.1.3.1 Application safety issues

Application layer mainly contains a variety of applications for example, industrial monitoring, smart grid, monitoring services, or any other intelligent system. The main security problem can be its own design flaws that can attract any attacker to attack. Malicious code or software vulnerabilities can be introduced in such defected systems. Another issue can be the integration

of various areas of techniques and business needs which can cause a bottleneck for the massive data processing and on operation control this can lead to the security issues of reliability and safety for IOT. Some of the issues could be privacy protection technology, database access control, protection technology of secure electronic products, information leakage tracking technology and intellectual property of software .

3.2 Security Parameters

Based on the IOT security issues, the need of security is required for IOT system. Therefore looking at the traditional parameters of security demand it needs to build a safe internet system of things, which are as follows,

- Authenticity: Received information by a reader should be noticeable whether is sent from authenticated electronic tag or not.
- Confidentiality: Sensitive Information shall not be leak to any unauthorized reader by using an RFID electronic tag.
- Integrality: While transmitting the information to IOT, data integrity can ensure the originality of information. It should ensure that the information transmitting is not fabricated i.e not rewritten, copied or replaced by the attacker.
- Privacy: Privacy such as identity or commercial interest of an individual user should be protected by the secure IOT system.
- Availability: An authorized user can able to use various services provided by IOT and can prevent DOS attack for the availability of the services. DOS attack is major cause for threat to the availability.

3.3 Security Countermeasures

The Xu Xiaohui talked about the countermeasures for the security issues of IOT. Some of them as certification, access control, data encryption and cloud computing are discussed in this subsection.

3.3.1 Certification

Certification is a secure way of confirming the true identity of both the parties which communicate with each other. Hence by using Public Key Infrastructure (PKI), it is possible to achieve the strong authentication by two way public key certification for preventing authenticity and confidentiality of the IOT system. Notarization is another solution for security purpose. Notarization is a trusted third party i.e. a certificate authority that facilitates interactions between the users to assure the properties of data exchange .

3.3.2 Access Control

Access control is another mechanism which gives secure environment of IOT by limiting the access control for machines, objects or people which are illegal to access the resources. Certification and access control technology are correlated with each other. For correct access control, IOT should ensure the correct identification by certification technique. Access control can be implemented on the area such as: Encrypt password, confidential directories or files, configuration and update rights etc. Designing a secure key Agreement scheme to restrict the key information to be attacked on can be helpful for it.

3.3.3 Data Encryption

Encryption technique is used to prevent the information from tampering and to maintain confidentiality as well as integrity of the information. When data is intercepted by an attacker, encryption prevents that data from being deciphered. There are two ways of Encryption:

Hop by Hop Encryption Provides cipher text conversion on each node to make it more secure for network layer.

End to End Encryption in which encryption-decryption performed at sender-receiver end only. According to the business needs, one can choose different encryption methods. Using more secure key exchange and key management schemes one can prevent attacks on IOT such as eavesdropping, fabrication, record and replay etc .

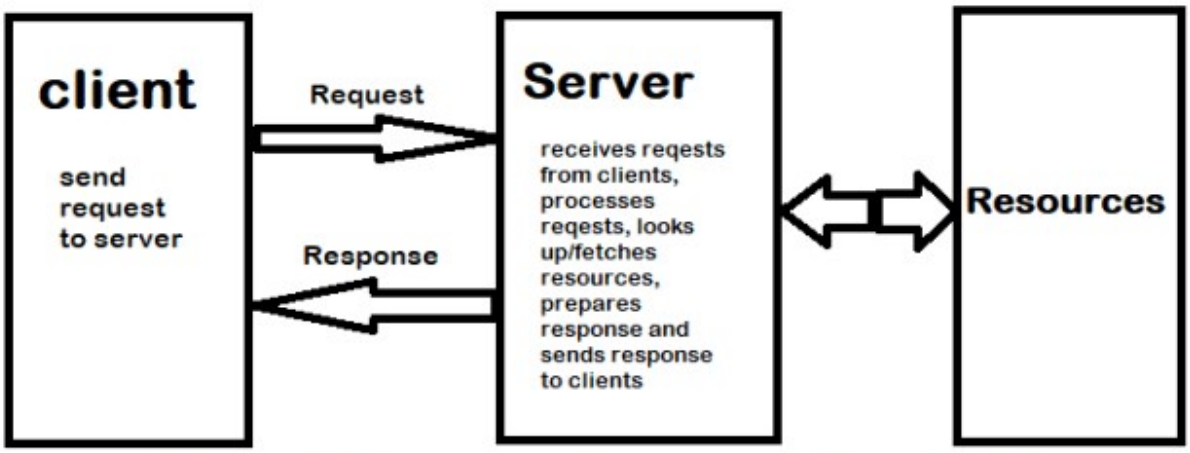
3.3.4 Cloud Computing

Cloud is a name for huge data storage capacity, high performance with affordable low cost. In the essential working of IOT i.e. large number of sensor nodes that collect and analyze huge amount of data, storing and processing of data where cloud computing can be used very effectively. Another use of cloud computing is providing third party security. IOT security can be enhanced using cloud‟s security at minimum cost, as cloud provides the feature of „pay for how much you use‟. While using cloud computing it needs to make sure that the „Scale‟ of IOT is large for example in areas such as, earthquake monitor, smart grid, industrial applications etc. . A summarized view of the working and security of IOT in Table 1 is given, and discussed about individual layer, components involved in the layer, working of each layer with its security issues and countermeasures.

IOT Communication models

IOT Communication models

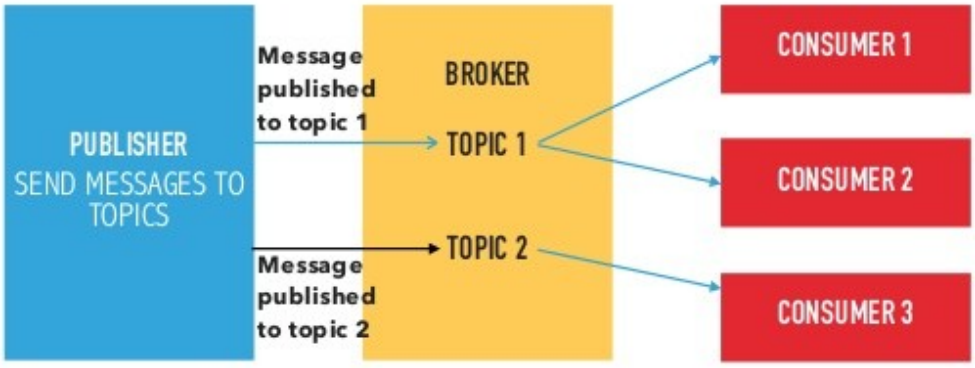
Request response model: The client is the IOT device that sends a request to the server. The request maybe for transfer of data or upload of data. The server maybe remote or local and can handle requests of multiple clients. The Request response model is stateless and hence each request is independently handled. Server can receive the request, decide its response and fetch the data.



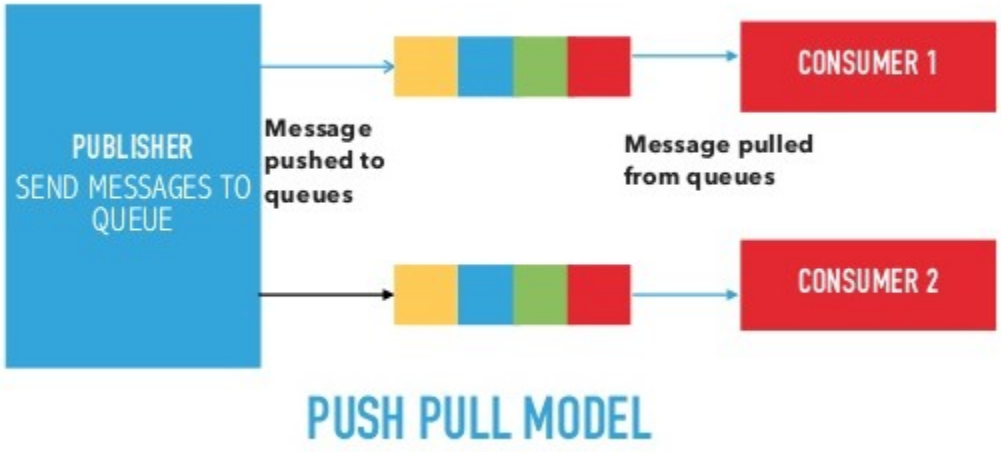
Request-Response Communication Model

Publish subscribe model: There are three entities publisher, broker and consumers. Publishers send the data to the brokers on topics managed by the brokers. Consumers subscribe to topics and brokers send the data on the topics to the consumers. Hence, brokers responsibility is to accept data from publishers and send it to the appropriate consumer.

PUBLISH SUBSCRIBE MODEL



Push-pull: Data producer push data to queues and consumer pull data from queues. Producers and consumers are not aware of each other. Queues act as buffers and are useful when producers produce data at a rate at which is faster than rate at which consumers can download.

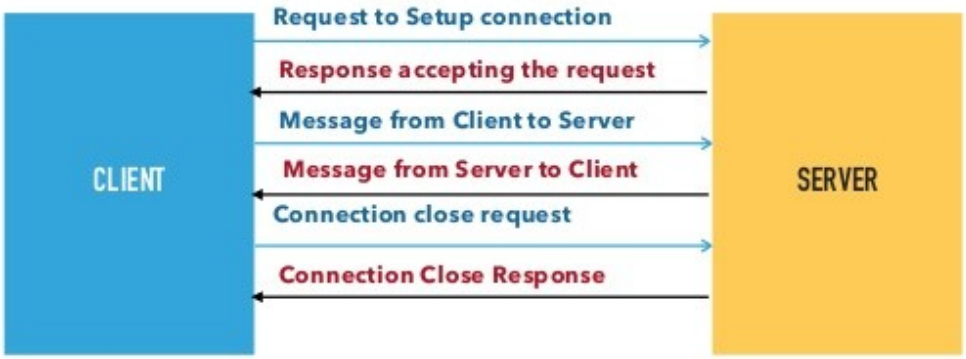


PUSH PULL MODEL

Exclusive pair: It is a bi-directional, full duplex commincation model that uses a persistent connection between client and server. The connection is persistent and remains open till client sends a request to close the connection. This is a stateful connection model and server is aware of all open connections.

COMMUNICATION MODELS

EXCLUSIVE PAIR COMMUNICATION MODEL



IOT Communication API - ReST

REST is acronym for REpresentational State Transfer. It follows request response model.

Guiding Principles of REST

Client–server – By separating the user interface concerns from the data storage concerns, we improve the portability of the user interface across multiple platforms and improve scalability by simplifying the server components. This means that the client user interface should not be concerned with the storage of data as that is looked after by server. Similarly, server should not be concerned with user interface which is handled by client.

Stateless – Each request from client to server must contain all of the information necessary to understand the request, and cannot take advantage of any stored context on the server. Session state is therefore kept entirely on the client.

Cacheable – Cache constraints require that the data within a response to a request be implicitly or explicitly labeled as cacheable or non-cacheable. If a response is cacheable,

then a client cache is given the right to reuse that response data for later, equivalent requests.

Uniform interface – Method of interaction between client and server should be uniform. All resources are identified by unique identifiers and these ID's are mentioned in the client requests. Based on the requested resource the client is provided a representation of the resource. It can update or modify this representation.

Layered system – The layered system style allows an architecture to be composed of hierarchical layers by constraining component behavior such that each component cannot "see" beyond the immediate layer with which they are interacting.

Code on demand (optional) – REST allows client functionality to be extended by downloading and executing code in the form of applets or scripts. This simplifies clients by reducing the number of features required to be pre-implemented.

Resource The key abstraction of information in REST is a resource. Any information that can be named can be a resource: a document or image, a temporal service, a collection of other resources, a non-virtual object (e.g. a person), and so on. REST uses a resource identifier to identify the particular resource involved in an interaction between components.

The state of the resource at any particular timestamp is known as resource representation. A representation consists of data, metadata describing the data and hypermedia links which can help the clients in transition to the next desired state.

Resource Methods- These are to be used to perform the desired transition

IOT Levels - Deployment Templates

IOT systems consist of following components:

Device: These may be sensors or actuators with capability of identifying, remote sensing or monitoring.

Resources: These are software components on IOT devices for accessing, processing, storing software components or controlling actuators connected to device. Resources also include software components that enable network access.

Controller service: It is a service that runs on the device and interacts with web services. Controller service sends data from the device to the web service and receives commands from the application via web services for controlling the device.

Database: Stores data generated from device

Web service: Provides a link between IOT device, applications, database and analysis components.

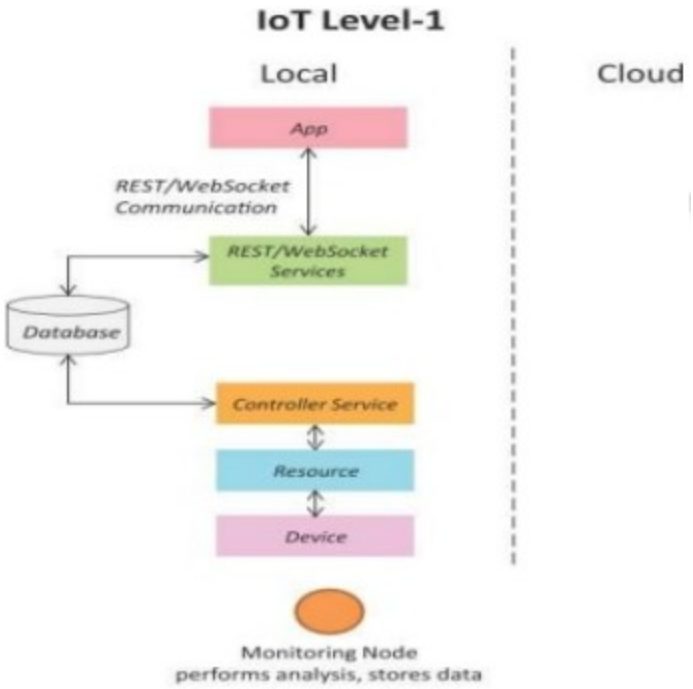
Analysis component: It performs analysis of the data generated by the IOT device and generates results in a form which are easy for the user to understand.

Application: Provides a system for the user to view the system status and view processed data. It also allows user to control and monitor various aspects of the IOT system.

IOT Levels

IOT level 1 - IOT system consists of a single node/ device that performs sensing or actuations , stores data , analyses it and hosts the application.

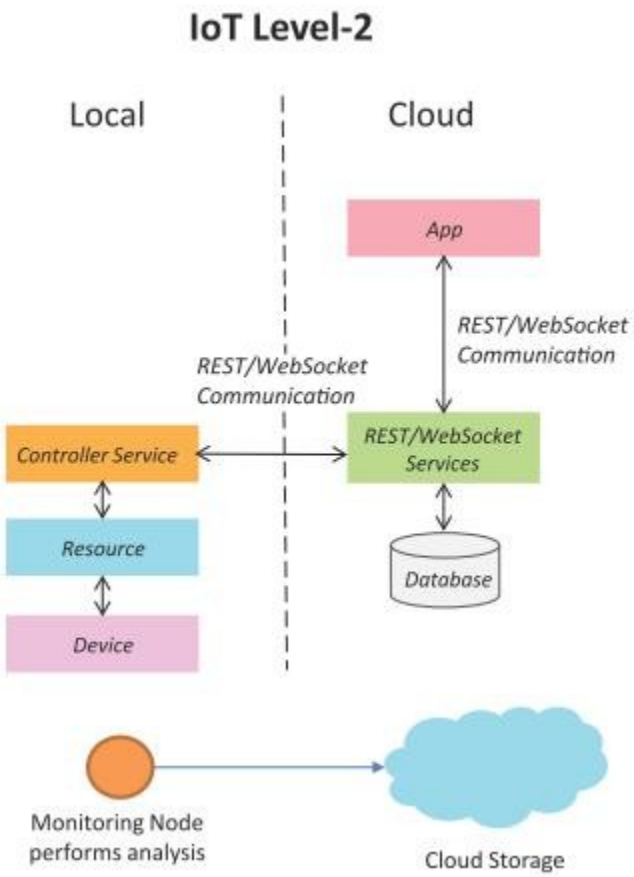
Example: Consider an IOT device that monitors the lights in a house. The lights are controlled through switches. Status of each light is maintained in a local database. REST services deployed locally allow retrieving and updating state of each light in the database and triggers the switches accordingly. Application has a user interface for controlling the lights or applications locally. Device is connected to the internet and hence the application can be accessed remotely as well.



IOT Levels

IOT level 2 - A node performs sensing / actuation and local analysis. Data is stored in the cloud.

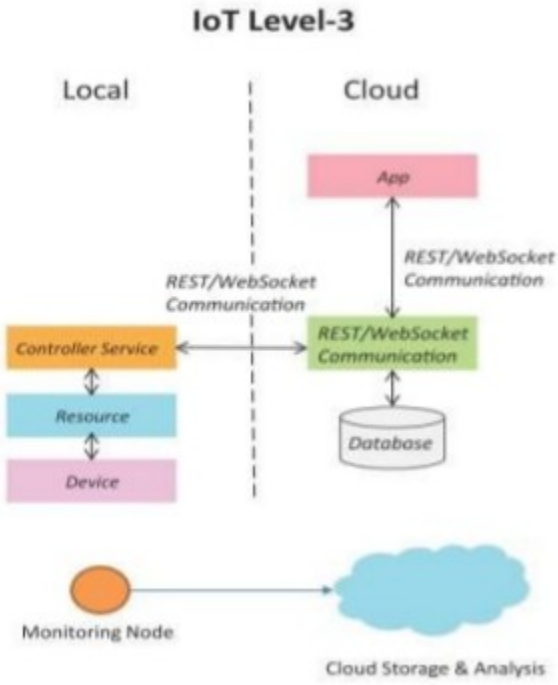
Example: A single node monitors the soil moisture in the field. This is sent to the database on cloud using REST APIs. Controller service continuously monitors moisture levels. Cloud based application is used for monitoring and controlling the IOT system.



IOT Levels

IOT level 3 -A single node monitors the environment and stores data in the cloud. Application is cloud based. This is suitable where data is voluminous and analysis is computationally intensive.

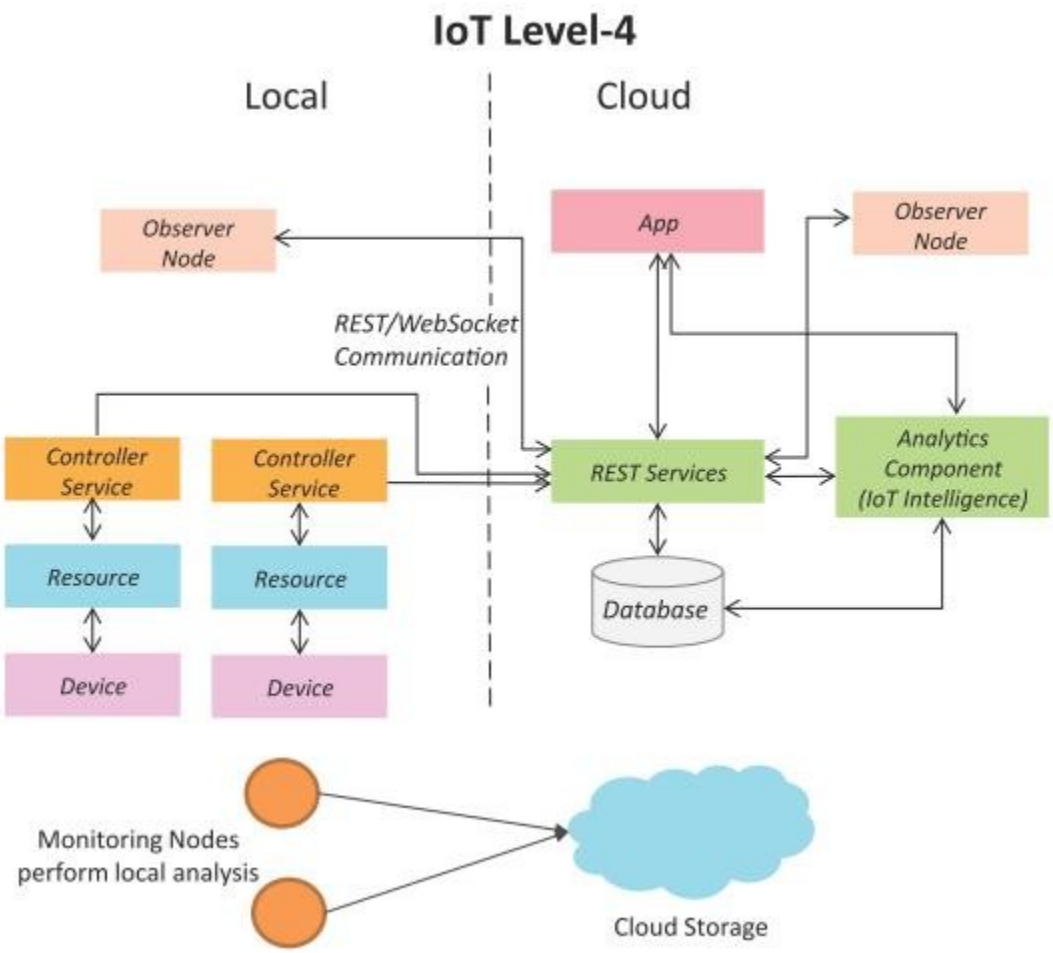
Example: A node is monitoring a package using devices like accelerometer and gyroscope. These devices track vibration levels. Controller service sends sends sensor data to cloud in real time using WebSocket API. Data is stored in cloud and visualised using cloud-based application. Analysis component triggers alert if vibration levels cross a threshold.



IOT Levels

IOT level 4 -Multiple nodes collect information and store in the cloud. A cloud based application controls the system. Local and remote observer nodes are present that subscribe to and receive information collected in cloud from various devices. Observer nodes can process information and use it for applications but do not perform control functions.

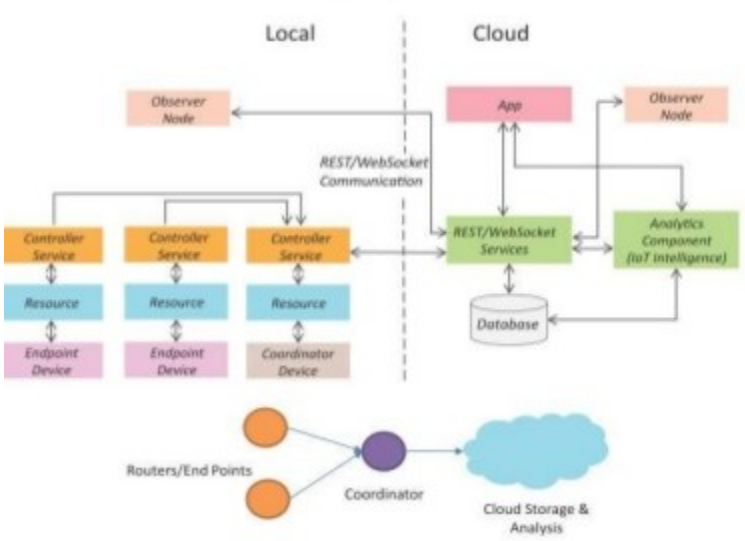
Example: Noise monitoring of a area requires various nodes functioning independent of each other. Each has its own controller service. Data is stored in cloud database. Analysis is done on the cloud and the entire IOT system is monitored on the cloud using an application.



IOT Levels

IOT level 5-Nodes present locally are of two types : end nodes and coordinator nodes. End nodes collect data and perform sensing or actuation or both. Coordinator nodes collect data from end nodes and sends it to cloud. Data is stored and analysed in cloud and application is cloud based.

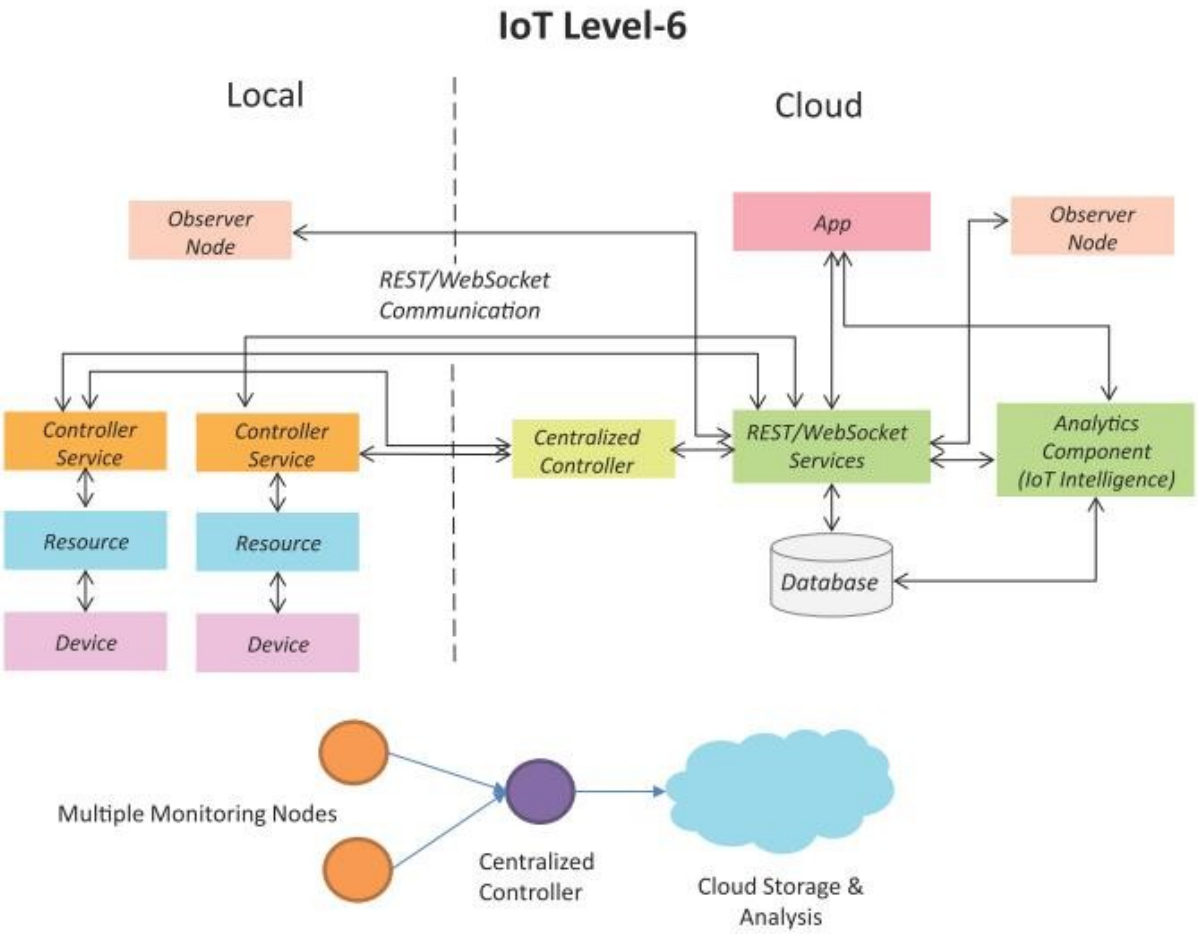
Example: A monitoring system has various components: end nodes collect various data from the environment and send it to coordinator node. Coordinator node acts as gateway and allows the data to be transferred to cloud storage using REST API. Controller service on the coordinator node sends data to the cloud.



IOT Levels

IOT level 6- Multiple independent end nodes perform sensing and actuation and send data to cloud. Data is stored in cloud and application is cloud based. The analytics components analyses the data and stores the results in the cloud database. The results are visualized with cloud based application. The centralized controller is aware of the status of all the end nodes and sends control commands to the nodes.

Example: Weather monitoring consists of sensors that monitor different aspects of a system. The end nodes send data to cloud storage. Analysis component, application and storage are in cloud. Centralized controller controls all nodes and provides inputs.



Unit 2 Chapter 2
Design of Smart Traffic Management System Using IoT

IoT platform has been widely applied for the development of intelligent transport system which resulted in the evolution of traffic control and prediction system. It is approaches that uses the mechanism of IoT for controlling the traffic and ensure safety [6]. The task is mainly achieved by the collection and analysis of the real time traffic data.

Objectives of Intelligent Transport System

The objectives of intelligent transport system are: i. Increasing the Efficiency of Transportation System ii. Mobility Enhancement iii. Ensuring Safety and Security iv. Reduction of Fuel Consumption v. Increasing Economic Productivity

Techniques Used In order to achieve the above mentioned objectives, the following methods are applied:

Detection of Inductive Loop Inductive Loops are used for transmitting signals with an aim to recognize objects using metal detector or vehicle indicator. A narrow ditchin the street is filled up with insulated cables which are connected to a controller The induction inside the wires changes depending on the number of number of vehicles crosses the wires or stops across them. This change in induction also changes the frequency which generates an electronic signal. This signal reaches the control unit and helps to detect the existence of vehicles. This signal is further analysed to find out the number of vehicles within that area and also track their movements.

Video Analysis

A smart camera with a data processor, stimuli sensitive sensors and a transmission unit is used for this purpose . The camera is used to capture video which is used for calculation of the traffic statistics resulting in exposure of certain information like vehicle frequency, path occupancy and average speed. However this scheme needs high investment cost and proper Street lightening during nights.

Infrared Sensors

Infrared sensors can sense any kind of infrared radiation. They capture the energy emitted from vehicles and road surface which is converted to electrical impulses using infrared reactive objects. These stimuli can be used for traffic checking, signal management, recognition of pedestrians etc. However, infrared sensors can become ineffective due to smoke and fog. The installation and maintenance of these devices is also quiet complex [

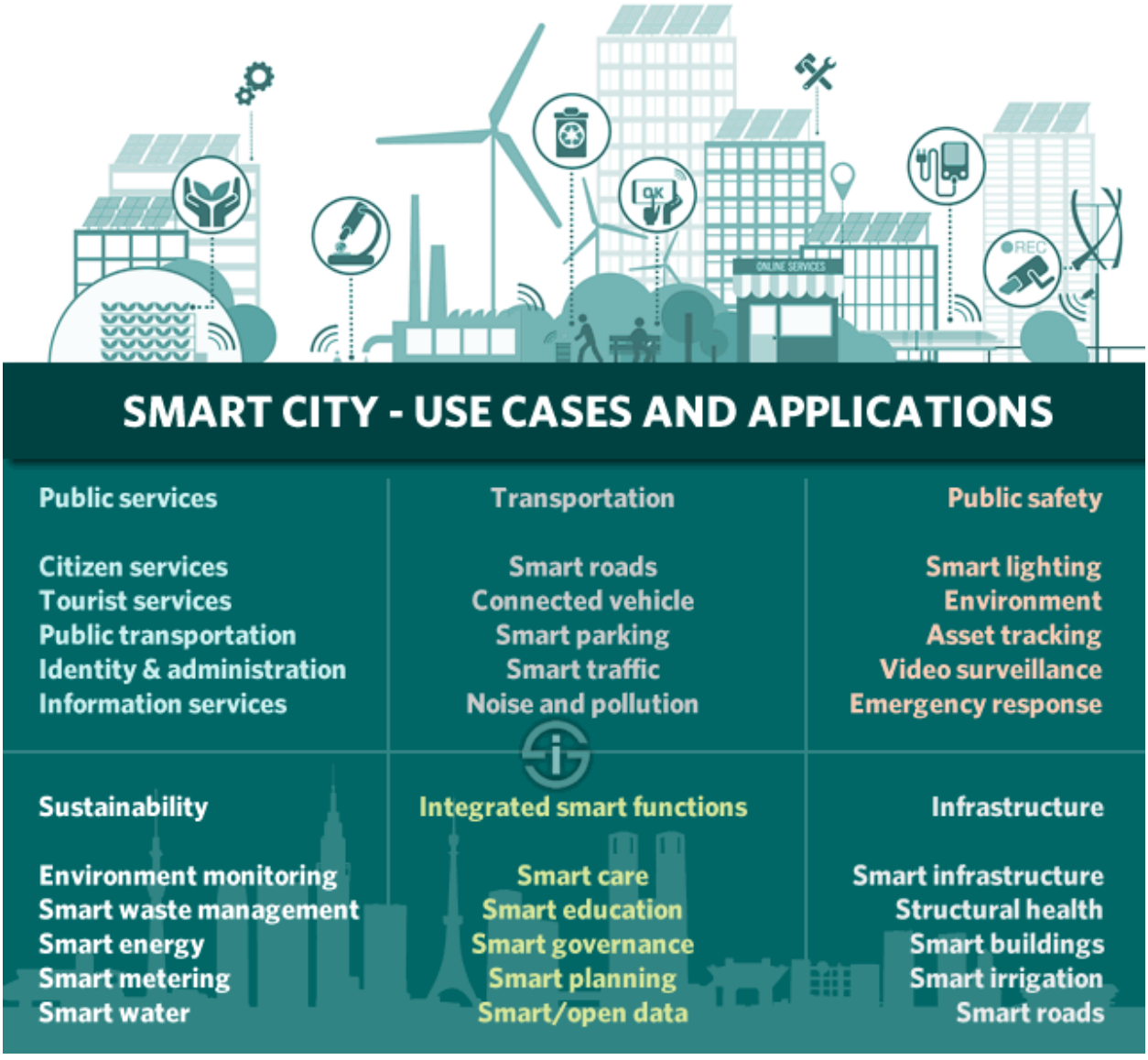
Wireless Sensor Network

Wireless sensors are often employed for detection of traffic to avoid the road congestion. They can transfer information very fast, are easy to install, require less maintenance, and are compact and cheaper than other electronic devices [8, 10, 11]. They can be used to ensure priority for emergency vehicles. Research is going on to monitor and control the real time traffic using Wireless Sensor Network in combination with Bluetooth devices and cameras.

Design of the Traffic Management System RFID tag is deployed with the vehicles which hold data about the vehicles. The tag can be used to identify other vehicles. IT describes how the real traffic is subjected to the detection system and thereby passed to the control decision.

Smart cities and citizen-facing public services
Probably the best-known usage of the Internet of Things in a government context concerns smart cities, in reality mainly smart city applications.

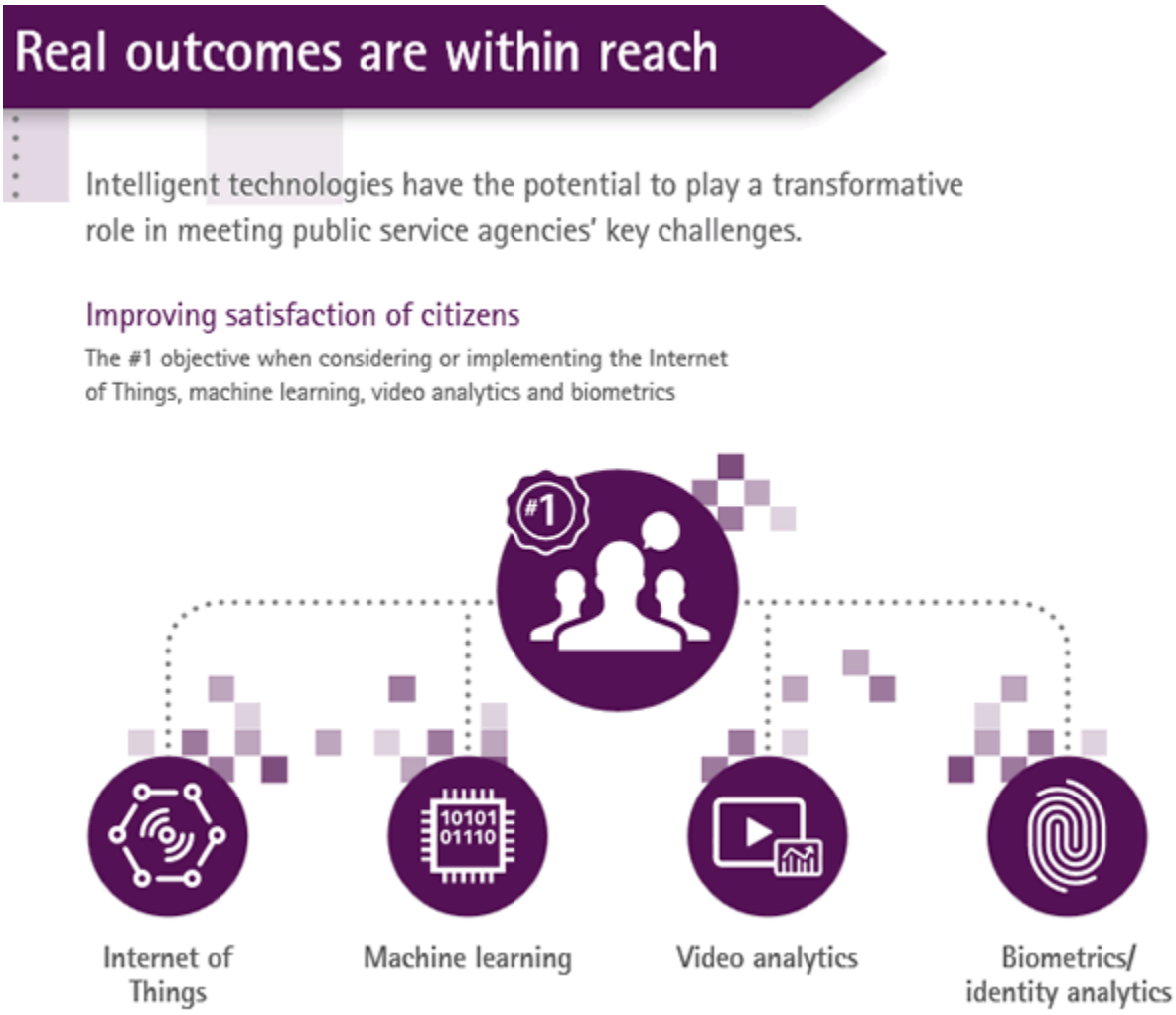
Smart city projects are what people hear about most and they get a lot of attention, among others because smart city applications are close to the daily lives of residents. Another reason why smart cities are often mentioned is that de facto smart city projects account for a big portion of Internet of Things deployments. Think about smart waste management *(often a local matter)*, smart parking and environment monitoring.



More about smart cities

Another area where we see the Internet of Things popping up is in citizen-facing public services.

To a large extent smart city uses cases overlap with Internet of Things use cases in public services as one of the key tasks of a city is to serve the citizens. However, with public services we also go beyond the local/urban level. The degree of overlap depends on the way government services are organized in a particular country or region. Internet of Things initiatives in citizen-facing public services include the already mentioned local ones but also smart energy *(often with state-sponsored partners)*, for instance.



Improving citizen satisfaction is the main objective when considering or implementing the Internet of Things and other emerging technologies – source Accenture infographic

IoT and public services

Infrastructure, healthcare, safety and security

Public services brings us to infrastructure. Again, this is a broad category which can be organized by several partners in the government ecosystem. Smart grid is an example, smart roads another one *(in cases where road infrastructure is a national or 'shared' matter)*. But also think about applications such as toll collection.

Next there is safety and security. On a national level this certainly also includes defense and the industrial-military complex. On more regional levels we see applications such as smart lighting *(there is a link between lighting of public spaces and crime)*, various forms of identity control, surveillance and so on. Last but not least, there is the role of the Internet of Things in security alerts, fighting natural disasters etc.

That brings us to healthcare, another sector going through digital transformation, and closely related with government. Healthcare is organized differently across the globe, from funding to healthcare insurance and actual care. However, there is always a government component. Healthcare is a key Internet of Things market.

Moreover, governments have a role in public health which can be enhanced by taking initiatives using the Internet of Things and in collaboration with private an state-sponsored partners. The same goes for public safety by the way. An example: collaborations between governments and insurance firms, leveraging telematics.

The omnipresence of the Internet of Things in government – opportunities, regulation and challenges

There are really hundreds of ways in which governments leverage and can leverage the Internet of Things to improve citizen experience, realize cost savings and, not to forget, generate new revenue streams.

The latter is quite important as many IoT projects have an impact on the funding of cities. A simple example: if you have a perfectly working smart parking solution in a city, you lose revenues for all the obvious reasons. So, it's not just a matter of technologies but also of finding creative ways to turn enhanced citizen experience and citizen services in a global picture that is beneficial for everyone.

This takes time, planning and, as you can imagine, given the complexity of the government ecosystems, lots of alignment and coordination.

In some countries and on supra-national levels initiatives are taken and funding is foreseen across a range of ‘smart’ initiatives where often also cities and government agencies can benefit from in the scope of projects within a designated area and an agenda with a clear goal. At the same time, governments get increasingly active in the area of Internet of Things security and regulation, as said, is always nearby. As an example, take the connected car of the future. It’s pretty clear that governments will be hugely involved in this and it’s less obvious than it may seem. Just to give you an idea: in some countries, traffic regulations are already a complete mess because of the arrival of fast electrical bikes. You can imagine what will happen once vehicles are connected and ‘smart’.

The Internet of Things in buildings and facilities

The Internet of Things plays an important role in facility management, among others including smart buildings.

The integration of IT (Information Technology) and OT (Operational Technology) plays an important role in this regard as it did in the fast rise of Industrial Internet of Things. Thanks to the Internet of Things and this IT/OT convergence, facility managers and building professionals can realize various goals. These depend on the nature and scope of the facility/building.

Smart buildings are among the fastest growing cross-industry Internet of Things use cases in the period until 2020. Moreover, research indicates that data collection from buildings and other structures such as HVAC is already high. Last but not least, the market and evolutions of the BMS (Building Management System) are strongly impacted by the Internet of Things. According to research, the Internet of Things is one of the dominant drivers in both spending and evolutions in the BMS market, which is forecasted to grow at a CAGR of 16.7 percent between 2017 and 2023 according to one of the many studies regarding that BMS market.

As the graphic below indicates, building management systems are becoming the centers of connectivity in a world of ever more endpoints in buildings which are leveraged by several building management systems but whereby the BMS plays a central and connecting role as in the end it’s all about analytics and actions, whereby the building owner wants a central platform which the BMS will be and de facto already largely is.

BUILDING IOT ENDPOINT DATA COLLECTION & ANALYTICS AND THE BMS

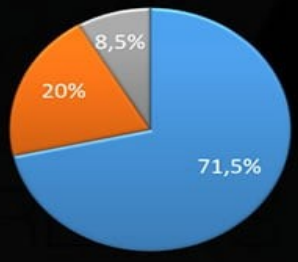
Data analytics and actionable data play a key role in the evolution of building design, the connected building and building management. As data collection from endpoints increases and next generation technologies make analytics and insights key in building systems, the connected BMS becomes a center of visualization, insights and action.

Data collection from equipment, devices or connected endpoints 2016

Top 5 IoT data collection points

1. Datacenter IT equipment
2. Cameras & Surveillance Equipment
3. Datacenter Facilities Equipment
4. Smartphones and End User Devices
5. Buildings and Other Structures (HVAC, etc.)

Types of sensing data collected by endpoints



Source: 451 Research - https://451research.com/images/Marketing/press_releases/06.29.16_VOTE_IoT_Q1_FINAL.pdf

Increase of data collection endpoints and analytics in buildings 2018 and beyond

Drivers of data collection and analysis growth from buildings

- Strong increase of smart building use case IoT spending (IDC)
- Demand of building owners and regulators for actionable data and analytics
- Expanded usage of IoT - towards the edge and field level
- Growing importance of IoT and analytics in all building systems: BMS, energy, lighting and room control, critical power, etc.
- Increasing usage of IoT and actuators on levels of devices and applications such as radiator, airflow, etc.
- Focus on autonomous decision making in building optimization with BMS as hub

The Internet of Things in buildings and facilities

The Internet of Things plays an important role in facility management, among others including smart buildings.

The integration of IT (Information Technology) and OT (Operational Technology) plays an important role in this regard as it did in the fast rise of Industrial Internet of Things. Thanks to the Internet of Things and this IT/OT convergence, facility managers and building professionals can realize various goals. These depend on the nature and scope of the facility/building.

Smart buildings are among the fastest growing cross-industry Internet of Things use cases in the period until 2020. Moreover, research indicates that data collection from buildings and other structures such as HVAC is already high. Last but not least, the market and evolutions of the BMS (Building Management System) are strongly impacted by the Internet of Things. According to research, the Internet of Things is one of the dominant drivers in both spending and evolutions in the BMS market, which is forecasted to grow at a CAGR of 16.7 percent between 2017 and 2023 according to one of the many studies regarding that BMS market.

As the graphic below indicates, building management systems are becoming the centers of connectivity in a world of ever more endpoints in buildings which are leveraged by several building management systems but whereby the BMS plays a central and connecting role as in the end it's all about analytics and actions, whereby the building owner wants a central platform which the BMS will be and de facto already largely is.

BUILDING IOT ENDPOINT DATA COLLECTION & ANALYTICS AND THE BMS

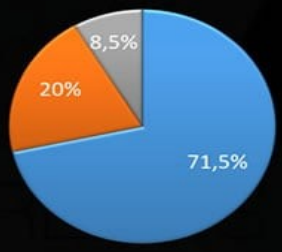
Data analytics and actionable data play a key role in the evolution of building design, the connected building and building management. As data collection from endpoints increases and next generation technologies make analytics and insights key in building systems, the connected BMS becomes a center of visualization, insights and action.

Data collection from equipment, devices or connected endpoints 2016

Top 5 IoT data collection points

1. Datacenter IT equipment
2. Cameras & Surveillance Equipment
3. Datacenter Facilities Equipment
4. Smartphones and End User Devices
5. Buildings and Other Structures (HVAC, etc.)

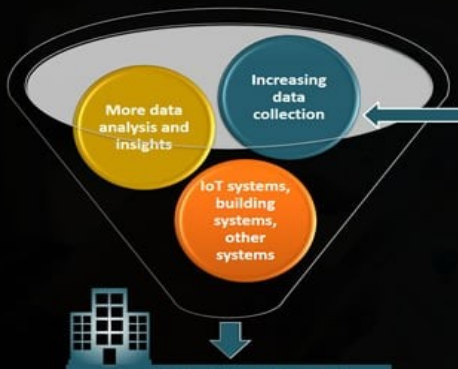
Types of sensing data collected by endpoints



- Machine sensing
- Environmental sensing
- Biological sensing

Source: 451 Research - https://451research.com/images/Marketing/press_releases/06.29.16_VOTE_IoT_Q1_FINAL.pdf

Increase of data collection endpoints and analytics in buildings 2018 and beyond



BMS fed by insights + data and connecting with other building systems and systems of insight and action

Drivers of data collection and analysis growth from buildings

- Strong increase of smart building use case IoT spending (IDC)
- Demand of building owners and regulators for actionable data and analytics
- Expanded usage of IoT - towards the edge and field level
- Growing importance of IoT and analytics in all building systems: BMS, energy, lighting and room control, critical power, etc.
- Increasing usage of IoT and actuators on levels of devices and applications such as radiator, airflow, etc.
- Focus on autonomous decision making in building optimization with BMS as hub

Building management systems

Leveraging data from IoT-enabled facility assets, along with new Internet of Things platforms and facility management, with embedded capabilities, are leading to possibilities and benefits in building management areas such as:

- Smarter building security systems.
- Smarter Heating, ventilation and air conditioning (HVAC).
- Safer and more comfortable/healthy workplaces and buildings.
- Facility service quality optimization.
- Cost reductions, also in a green building context and in reduction of energy and water consumption.
- Better planning, operational efficiencies and enhanced resource allocation.
- Predictive maintenance and facility maintenance planning.
- Facility equipment control, configuration and regulation.
- Building management and building automation.
- Energy efficiency.
- Light and room control, comfort.

This list is far from comprehensive. As there are various sorts of buildings, each with their own challenges, infrastructure, technologies and most of all goals the landscape of building automation and management is very broad.

In light and room control alone there are several controls such as blind controls, AC unit controls and literally dozens more.

The overall building automation and management landscape exists since far before the Internet of Things existed and is composed of various specializations, each with their standards *(e.g. KNX in room control or BACnet in building management systems)*, certification programs for green buildings *(ecology and energy/ecology regulations are key drivers*) and for OT channel partners, technologies, networks, solutions and of course goals *(the goal of an IoT-enabled office space, building or even meeting room is not the same of a hospital, even if there are always overlaps)* .

However, with the Internet of Things these worlds are converging *(and the standards already evolved to IP)*. This is a challenge and opportunity for the various players who all have their skillsets but rarely are able to offer the full picture.

HVAC, for example, requires entirely different capabilities than power management or building management systems. That's why companies like Schneider Electric have developed partner and

system integrator certification programs for various smart building specializations whereby the so-called EcoXperts *(EcoXpert is the name of the partner program)* can learn new skills, connect, expand into new domains and even go for multiple certification badges as the Internet of Things is increasingly dominating all building domains. Some of the players in these segments have a more mechanical background, others an electrical background and still others, such as system integrators, a background of customization and software (PLCs).

Among these providers we find:

- Light and room control experts.
- Experts in very specific areas such as HVAC.
- Players in the broader building management field, mainly in large buildings.
- Electrical contractors who are often more involved with smaller and medium buildings where they can offer smart energy solutions or, for instance specialize in home automation.
- Experts in critical power, which you typically find in airports, hospitals and other buildings where quality and reliability of power is critical in all senses.

Building management and Internet of Things

The Internet of Things in Healthcare

The Internet of Things has been present in healthcare in many forms and shapes since several years.

With remote healthcare monitoring and medical/hospital asset tracking, monitoring and maintenance as typical examples of these initial applications, the face of the Internet of Things in healthcare is changing fast.

Among the evolutions and drivers of the Internet of Things in healthcare:

- **An increasing consciousness and engagement from the consumer/patient side** leads to new models, leveraging personal healthcare devices.
- **In a more integrated perspective, data from biosensors, wearables and monitors are used in real-time health systems** and to save time for caregivers, detect patterns, be more aware and increase quality of care.
- **A broad range of innovations in fields such as smart pills and ever better delivery robots help in making healthcare more efficient** and in saving resources, while also increasing quality of care.

Whether it’s on the level of caregivers and healthcare providers, healthcare payers, the pharmaceutical industry, the patient (who should come first and demands it) or other

stakeholders in the broader healthcare picture: we are moving from ad hoc and early Internet of Things deployments and use cases to a far more important role of the Internet of Everything in healthcare.

The graphic below shows the importance of remote monitoring as the main use case in healthcare from a spending perspective until 2020 and ongoing growth in the years after that with some vital sign monitor devices, followed by ways how healthcare providers and healthcare payers plan to leverage the Internet of Things and, finally smart healthcare market growth data, based on IDC, Technavio and Grand View Research.

INTERNET OF THINGS IN HEALTHCARE

2017 - 2020

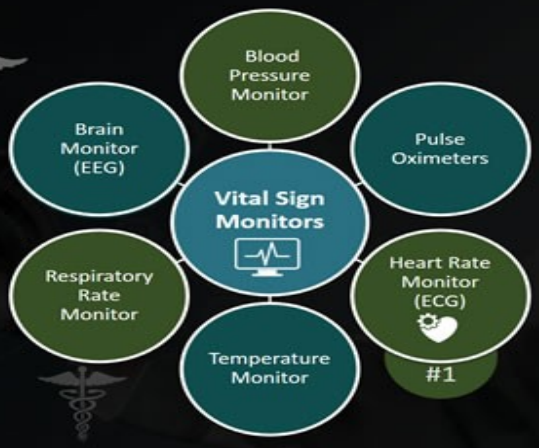
REMOTE MONITORING

"Remote health monitoring will see the greatest investment in the Healthcare industry" (2020, IDC)

+40% of organizations IoT-enabled biosensors by 2019

Remote Patient Monitoring Devices Market

- Increased use of remote patient monitoring will help drive global smart healthcare market at a CAGR of 24.55% by 2020 (Technavio)
- Global remote patient monitoring devices market is expected to reach USD 1.9 billion by 2025 at a CAGR of 13.4% (Grand View Research)



HEALTHCARE IOT FORECASTS PROVIDERS & PAYERS

Healthcare providers

ROBOTS
By 2019, there will be a 50% increase in the use of robots to deliver medications, supplies, and food throughout the hospital

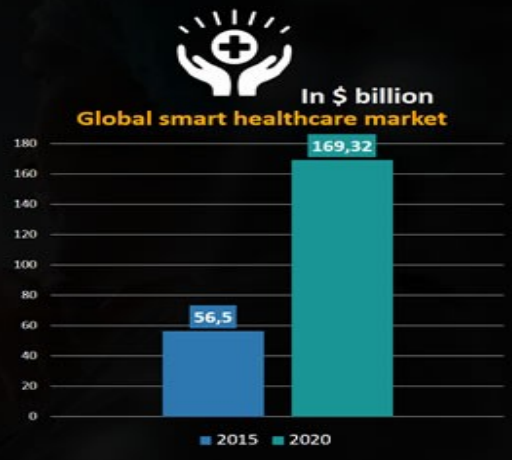
PATTERNS
By 2019, 60% of healthcare applications will collect real-time location data and clinical IoT device data and embed cognitive capabilities to discover patterns, freeing up 30% of clinicians' time

Healthcare payers

ACTIVE ENGAGEMENT
The Internet of Things and wearables play a role in the move from passive to active patient engagement, which takes place in 2017.

RPA
By the end of 2018, payers will have saved $1 Billion through implementation of Robotic Process Automation (RPA) tools, skill sets, and process reengineering.

SMART HEALTHCARE



Sources

IDC FutureScape: Worldwide Healthcare IT 2017 Predictions
Visit https://www.idc.com/research/viewtoc.jsp?containerId=US41864316

IDC Survey: Payer and Provider Investment Plans for Digital Transformation
Visit https://www.idc.com/getdoc.jsp?containerId=US42298217

Smart Healthcare – Technavio Top Market Drivers and Trends
Visit http://ow.ly/TV6C30ashvl

Remote Patient Monitoring Devices Market (Grand View Research)
Visit http://www.grandviewresearch.com/industry-analysis/remote-patient-monitoring-devices-market

Some evolutions and forecasts in healthcare IoT in numbers:

- **Research shows that by 2019, 89% of all healthcare organizations will have adopted IoT** technology and that the Internet of Things will be essential in the initiatives of healthcare payers and providers in 2017 and 2018.
- **Among the main perceived benefits of healthcare IoT** in the future are increased workforce productivity (57%), cost saving (57%), the creation of new business models (36%) and better collaboration with colleagues and patients (27%). The key benefits as reported in March 2017, however, are increased innovation (80%), visibility across the organization (76%) and cost savings (73%).
- **Other research shows that wearables will play a key role in health care plans**, clinical IoT device data will free up clinician's time significantly by 2019 (up to 30%) and there will be an increasing role for IoT-enabled biosensors and robots for medication and supplies delivery in hospitals by 2019 as the graphic below shows.

More data, use cases and evolutions regarding the Internet of Things in healthcare via the button below.

Internet of Things in healthcare