Smart City

- smart city is an urban area that uses different types of electronic methods and sensors to collect data. Insights gained from that data are used to manage assets, resources and services efficiently; in return, that data is used to improve the operations across the city.
- This includes data collected from citizens, devices, buildings and assets that is then processed and analyzed to monitor and manage traffic and transportation systems, power plants, utilities, water supply networks, waste, crime detection, information systems, schools, libraries, hospitals, and other community services.[

An IoT Strategy for Smarter Cities:

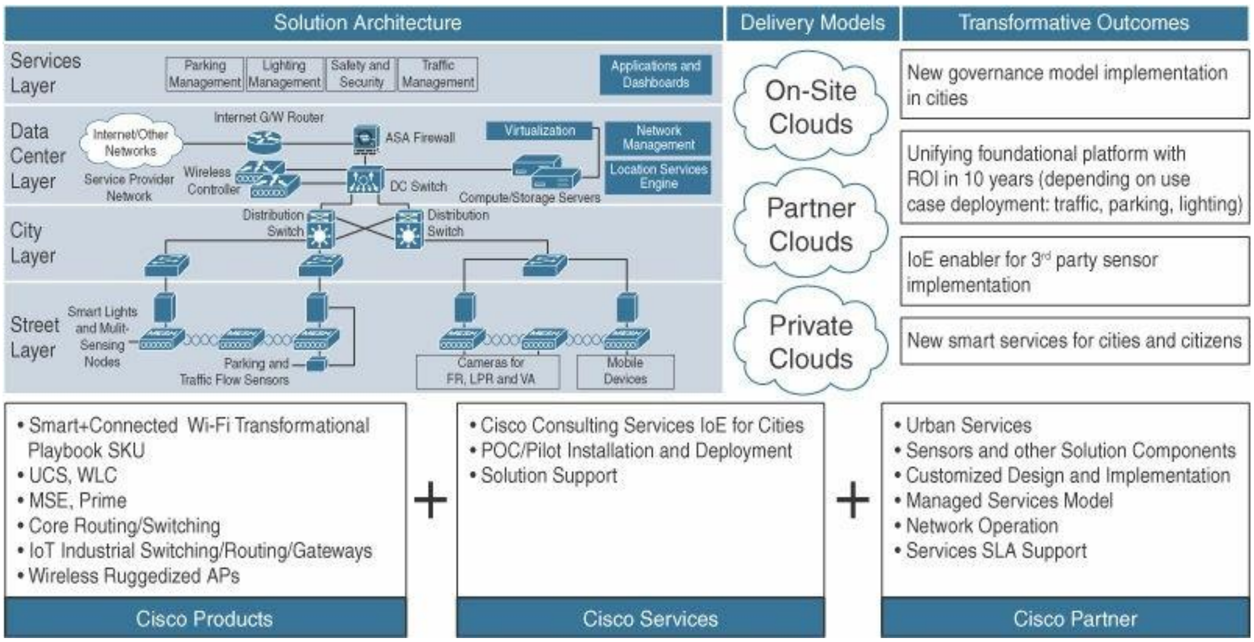
- IoT technologies can be leveraged to improve the lives of citizens and the efficient management of urban centers.
- There are many different approaches and solutions for city management. All these solutions typically start at street level, with sensors capture data on everything from parking space availability to water purity.
- Information and communications technology connects people, data, things, and processes together in networks of billions or even trillions of connections. These connections create vast amounts of data, some of which has never been accessible before.

A recent CISCO study, expects IoT to have the following economic impact over a 10-years period.

- **Smart buildings:** Smart buildings have the potential to save $100 billion by lowering operating costs by reducing energy consumption through the efficient integration of heating, ventilation, and air-conditioning (HVAC) and other building infrastructure systems.
- **Gas monitoring:** Monitoring gas could save $69 billion by reducing meter-reading costs and increasing the accuracy of readings for citizens and municipal utility agencies. The financial benefit is obvious for users and utility companies when the utility is managed by the city. There are also very important advantages in terms of safety, regardless of who operates the utility. In cases of sudden consumption increase, a timely alert could lead to emergency response teams being dispatched sooner, thus increasing the safety of the urban environment.
- **Smart parking:** Smart parking could create $41 billion by providing real-time visibility into parking space availability across a city. Residents can identify and reserve the closest available space, traffic wardens can identify noncompliant usage, and municipalities can introduce demand-based pricing.
- **Road pricing:** Cities could create $18 billion in new revenues by implementing automatic payments as vehicles enter busy city zones while improving overall traffic conditions. Real-time traffic condition data is very valuable and actionable information that can also be used to proactively reroute public transportation services or private users.

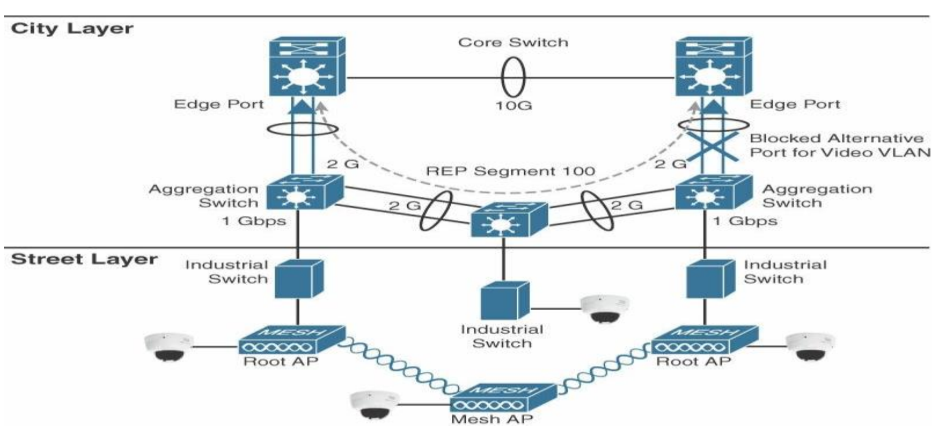
- **Water management:** Smart water management could save $39 billion by connecting household water meters over an IP network to provide remote usage and status information. The benefit is obvious, with features such as real-time consumption visibility and leak detection. In addition, smart meters can be used to coordinate and automate private and public lawn watering, initiating the watering programs at times when water consumption is lower or in accordance with water restrictions imposed by civic authorities.

Smart Cities Layered Architecture:



It is a four- layered Architecture,
Here Data flows from devices at the street layer to the city network layer and connect to the data center layer, where data is aggregated, normalized, and virtualized.The data center layer provides information to the service layer, which consists of the applications that provide services to the city.

Street Layer:



The street layer composed of devices and sensors that collect data and take action based on instructions from the overall solution, as well as the networking components need to aggregate and collect data.

A variety of sensors are used at the street layer for a variety of smart city use cases some of them are :

- **A magnetic sensor** can detect a parking event by analyzing changes in the surrounding magnetic field when a heavy metal object, such as a car or a truck, comes close to it (or on top of it).
- **A lighting controller** can dim and brighten a light based on a combination of time-based and ambient conditions.
- **Video cameras** combined with video analytics can detect vehicles, faces, and traffic conditions for various traffic and security use cases.
- **An air quality sensor** can detect and measure gas and particulate matter concentrations to give a hyper-localized perspective on pollution in a given area.
- **Device counters** give an estimate of the number of devices in the area, which provides a rough idea of the number of vehicles moving or parked in a street or a public parking area or even of birds in public parks or on public monuments—for cities where bird control has become an issue.

For each type of data to collect, there are a variety of solutions and possible approaches are there.

The choice of sensor technology:

- It depends on the exact nature of the problem, the accuracy and cost trade-offs appropriate for it, and any installation limitations posed by the physical environment. Another consideration is the requirement to interact with other IoT systems in the same physical space.
- For example, parking space availability sensors may be part of a closed system available to users through an app, or they may have to interact through open APIs with other systems, such as towing companies, public law enforcement agencies, parking meters, and so on.

One of the key aspects to consider when choosing a sensing device is its lifetime maintenance costs.

- Some sensors are mounted on city infrastructure, such as light poles. These sensors can benefit from the power, and possibly the network connectivity, of their mounting location.
- However, other sensors may be installed in the ground or in other inaccessible locations. Once they are installed, the cost of pulling them out to deal with an issue is very high. Such sensors are normally battery operated and energy efficient so they have long life expectancy, and they are ruggedized to avoid maintenance costs.

Another key aspect to consider when choosing the right technology for a smart city is edge analytics.

Many sensors and their data must be managed through the network in a way that securely processes data with minimal delay—and often in real time. Distinguishing between events in order to send only relevant pieces of data is a key component with the large data intakes inherent in a smart city's design.

- For example, a **car-counting sensor** does not need to send an update for each car detected; it may send only a cumulative count every minute.
- Similarly, a pollution sensor may process chemical sensing all the time but send status reports only at intervals.

To maximize processing speed and minimize server requirements, the amount of data that goes through cloud servers must be event based.

Event-driven systems allow the city infrastructure to be contextually intelligent so that only targeted events trigger data transfer to the cloud.

- This flexibility allows the infrastructure to monitor a large number of systems without the risk of overloading the network with uneventful status update messages.
- Analytics processed on the edge distributes the computing and storage requirements for the cloud, maximizing data transfer speeds and minimizing server requirement and cost.

Finally, for sensor characteristics, storage is a key consideration that depends on the method, location, and length of time the data has to be archived.

- This varies based on legal requirements on a per-country basis as well as use case; the difference is significant between storing video for weeks and using a set of event based triggers, and it has a big impact on the analytics that can be included in the limited physical capacity of the device.
- Cities must figure out the best approach to address their storage requirements as well as determine how long they need to keep their data, and choose devices appropriately based on those criteria.

Another issue that network planning must take into account is the required level of agnosticism of smart city networks.

- LoRaWAN is growing as a major protocol for smart city sensors, across multiple verticals. However, multiple use cases mean that multiple protocols may be deployed.
- Many sensors come with their own gateways that are compatible with their specific hardware like smart sensors.
- Smart city networks also have to make possible local analysis and closed-loop decision making, which also means that computing capacity at end nodes needs to be higher than for typical deployments.
- The size and complexity of the network grows with the size of the smart city deployment, as well as with the number and types of sensors utilized by the city.

The IoT network infrastructure is the backbone of any cohesive smart solution for a city; device connectivity is the key to the utility of digitized public services.

City Layer:

- At the city layer, which is above the street layer, network routers and switches must be deployed to match the size of city data that needs to be transported.

- This layer aggregates all data collected by sensors and the end-node network into a single transport network. The city layer may appear to be a simple transport layer between the edge devices and the data center or the Internet.

one key consideration of the city layer is that it needs to transport multiple types of protocols, for multiple types of IoT applications.

- Some applications are delay and jitter-sensitive, and some other applications require a deterministic approach to frame delivery. A missed packet may generate an alarm or result in an invalid status report.
- As a result, the city layer must be built around resiliency (capacity to recover quickly from difficulties), to ensure that a packet coming from a sensor or a gateway will always be forwarded successfully to the head end station as shown in above figure.
- The Street Layer Resiliency In this model, at least two paths exist from any aggregation switch to the data center layer. A common protocol used to ensure this resiliency is Resilient Ethernet Protocol (REP)

Data Center Layer:

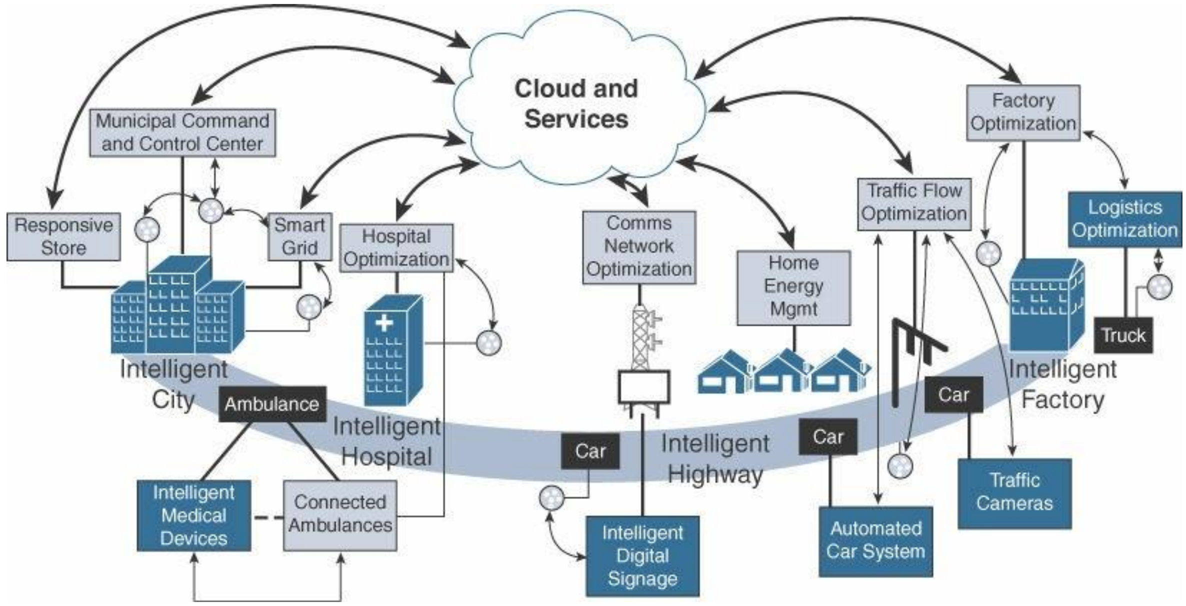
Ultimately, data collected from the sensors is sent to a data center, where it can be processed and correlated. Based on this processing of data, meaningful information and trends can be derived, and information can be provided back.

- For example, an application in a data center can provide a global view of the city traffic and help authorities decide on the need for more or less common transport vehicles. At the same time, an automated response can be generated.
- For example, the same traffic information can be processed to automatically regulate and coordinate the street light durations at the scale of the entire city to limit traffic congestion

The key technology in creating any comprehensive smart solution with services is the cloud.

- Traditional city networks simply cannot keep up with the real-time data needs of smart cities; they are encumbered by their physical limitations.
- The cloud enables data analytics to be taken to server farms with large and extensible processing capabilities.
- With a cloud infrastructure, data is not stored in a data center owned directly or indirectly by city authorities. Instead, data is stored in rented logical containers accessed through the Internet.
- The cloud provides a scalable, secure, and reliable data processing engine that can handle the immense amount of data passing through it.

- In addition, multiple contractors can store and process data at the same time, without the complexity of exclusively owned space as shown in bellow figure.
- This proximity and flexibility also facilitate the exchange of information between smart systems and allow for the deployment of new applications that can utilize the information from several IoT systems.



Edge or Fog Computing:

- However, not all data is processed in the central cloud-based data center. Most of the real-time and locally significant data can be directly processed at the edge of the network, leveraging a fog architecture.
- In this model, processing and analytics capabilities are made available at the top of the street layer, where gateways operate.
- In this way, data coming from multiple sensors (of the same type or of multiple different types) can be processed locally at the edge.
- Decisions are locally significant and can be made without unnecessary interactions with the cloud. The results from the locally processed data are then sent to the cloud to provide a more global perspective.

Service layer:

Smart city applications can provide value to and visibility for a variety of user types, including city operators, citizens, and law enforcement.

The collected data should be visualized according to the specific needs of each consumer of that data and the particular user experience requirements and individual use cases.

- For example, parking data indicating which spots are and aren't currently occupied can drive a citizen parking app with a map of available spots, as well as an enforcement officer's understanding of the state (utilization and payment) of the public parking space, while at the same time helping the city operator's perspective on parking problem areas in the city at any given time.

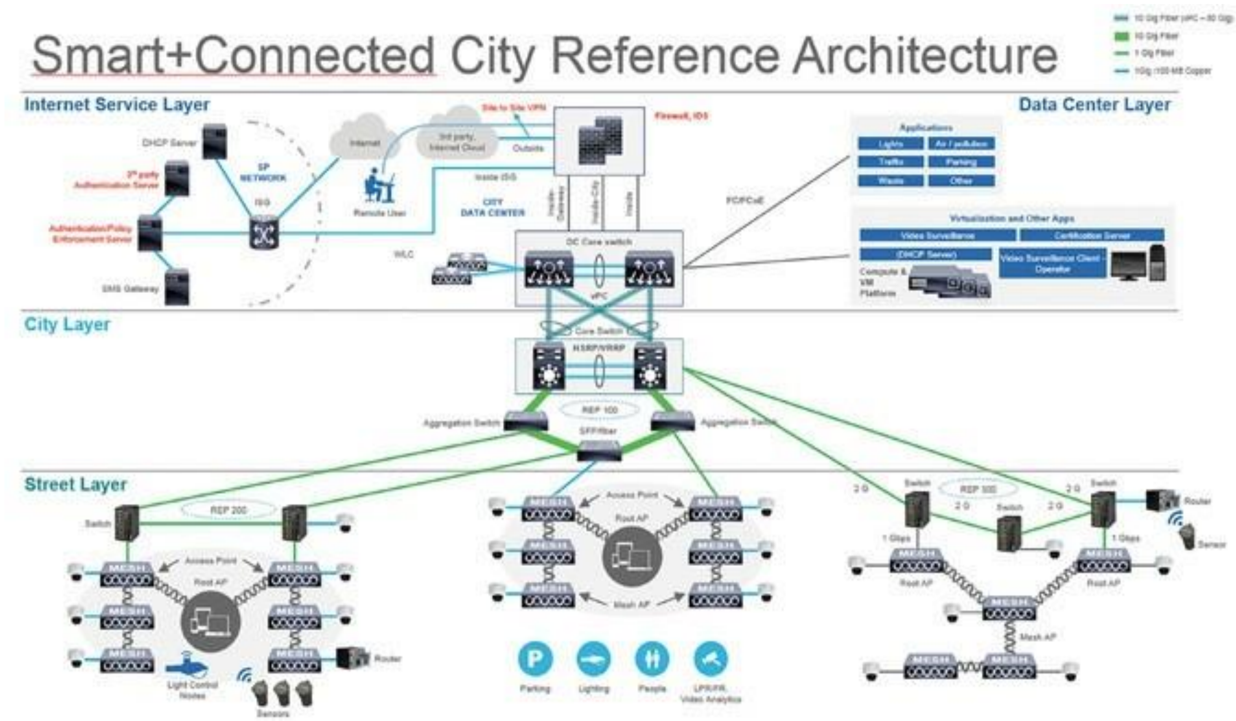
With different levels of granularity and scale, the same data performs three different functions for three different users. Along the same lines,

- The traffic information can be used by individual car drivers to find the least congested route.
- A variation of the same information can be made available to public transportation users to estimate travel times.

- Public transportation systems, such as buses, can be rerouted around known congestion points.

The architecture provides application developers and sensor vendors with the tools necessary to innovate and invent new community experiences via open APIs, software development kits (SDKs), city information models, and more to develop city-qualified applications that drive high-value smart city services.

Smart –Connected City Reference Architecture:



- The above figure shows a reference architecture, with specific security elements highlighted. Security protocols should authenticate the various components and protect data transport throughout.
- For example, hijacking traffic sensors to send false traffic data to the system regulating the street lights may result in dramatic congestion issues.
- The security architecture should be able to evolve with the latest technology and incorporate regional guidelines (for example, city by-laws, county or regionalsecurity regulations). Network partners may also have their own compliance standards, security policies, and governance requirements that need to be added to the local city requirements.

Smart City Use-Case Examples:

There are multiple ways a smart city can improve its efficiency and the lives of its citizens. The following sections examine some of the applications commonly used as starting points to implement IoT in smart cities:

- Connected street lighting
- Smart parking
- Smart traffic control
- Connected environment.

Smart parking:

Parking is a universal challenge for cities around the globe. According to urban planning researchers, up to 30% of cars driving in congested downtown traffic are searching for parking spaces.

Added traffic congestion is one consequence of drivers looking for parking space, and it has several consequences:

Contributes to pollution: Tons of extra carbon emissions are released into the city's environment due to cars driving around searching for parking spots when they could be parked.

Causes motorist frustration: In most cities, parking spot scarcity causes drivers to lose patience and waste time, leading to road rage, inattention, and other stress factors.

Increases traffic incidents: Drivers searching for parking spots cause increased congestion in the streets and that, in turn, causes increased accidents and other traffic incidents.

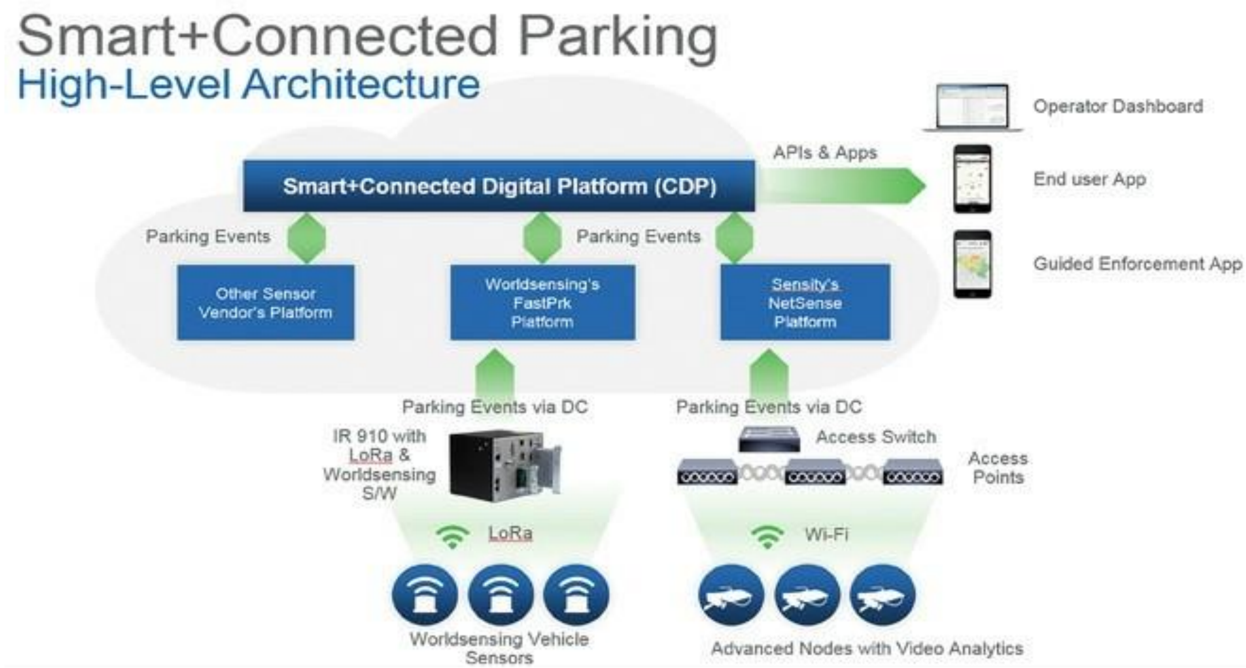
Revenue loss is another consequence of drivers looking unsuccessfully for parking space, and it also has various negative side effects:

Cities often lose revenue: As a result of inadequate parking meter enforcement and no parking, no-standing, and loading-zone violations, cities lose revenue.

Parking administration employee productivity suffers: Employees waste time roaming the streets, attempting to detect parking rules offenders.

Parking availability affects income: Local shops and businesses lose customers because of the decreased accessibility caused by parking space shortages.

Smart Parking Architecture:



Combining these technologies in innovative ways also expands the possibilities of the services IoT systems can deliver; this certainly holds true for smart parking.

- For example, sensors can be installed in disabled parking spots. An application can be used for drivers to register their disability and then locate these spots more easily.
- When a user parks, the sensor can communicate with the application on the driver's smart phone to validate the disability status and limit fraudulent use of these parking spaces.
- Regardless of the technology used, parking sensors are typically event-driven objects. A sensor detects an event and identifies it based on time or analysis.
- The event is transmitted through the device's communication protocol to an access point or gateway, which forwards the event data through the city layer.
- The gateway sends it to the cloud or a fog application, where it is normalized.
- An application shows the parking event on operator dashboards, or personal smart phones, where an action can be taken.
- For example, a driver can book a nearby parking spot, or a parking operator can remove it from the list of available parking spaces in target locations.
- This action triggers data to be sent back to the parking sensor to modify its availability status based on the received instructions.
- In turn, the sensor may interact with nearby systems. For example, in response to these instructions, lights above parking spaces can be turned red, orange, or green to display a free, booked, or occupied spot, thus facilitating a driver's search for an available parking spot.
- Similarly, a parking sensor can send a status to a general parking spot counter at the entrance of the parking deck to display how many spots are available in a given area, such as on a particular floor of a parking deck.

- This communication may be direct but often goes through a gateway, the network, and the application that communicates with the other systems through APIs.
- The user may also access the data from the cloud or fog-based applications to see the list of spots available in a particular city district or neighborhood.
- Smart data can also be embedded—for example, to increase the discount on more distant parking spots or increase the cost of parking spots closer to venues at particular times (such as sporting events or concerts).

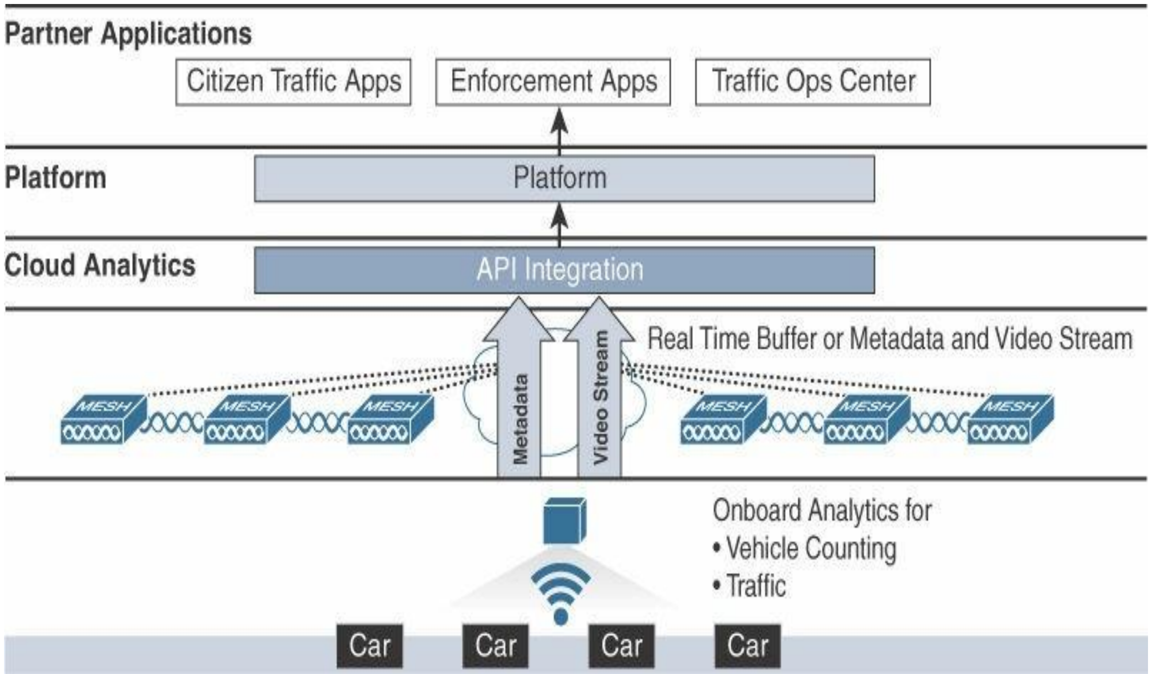
Smart parking has three users that applications must support through aggregated data:
city operators, parking enforcement personnel, and citizens. The true value of data normalization is that all parking data, regardless of technology or vendor, would be visible in these applications for the different users to support their particular experiences.
The following are some potential user experiences for these three user types:

- **City operators:**
  - These users might want a high-level map of parking in the city to maintain perspective on the city's ongoing parking situation.
  - They would also need information on historical parking data patterns to understand congestion and pain points in order to be able to effectively influence urban planning.
- **Parking enforcement officers**:
  - These users might require real-time updates on parking changes in a certain area to be able to take immediate action on enforcement activities, such as issuing tickets or sending warnings to citizens whose time is nearing expiration.
  - Their focus is driving revenue creation for the city and minimizing wasted time by performing parking monitoring and enforcement at scale.
- **Citizens:**
  - These users might want an application with a map (such as a built-in parking app in their car) showing available parking spots, reservation capabilities, and online payment.
  - Their focus would be on minimizing the time to get a parking spot and avoiding parking tickets. The application could warn when parking duration limits approach, allowing the driver to move the vehicle before the timer expires or pay a parking timer extension fee without having to go back to the vehicle.

Smart traffic control:

A smart city traffic solution would combine crowd counts, transit information, vehicle counts, and so on and send events regarding incidents on the road so that other controllers on the street could take action.

Smart Traffic Control Architecture:



In the architecture shown in bellow Figure,

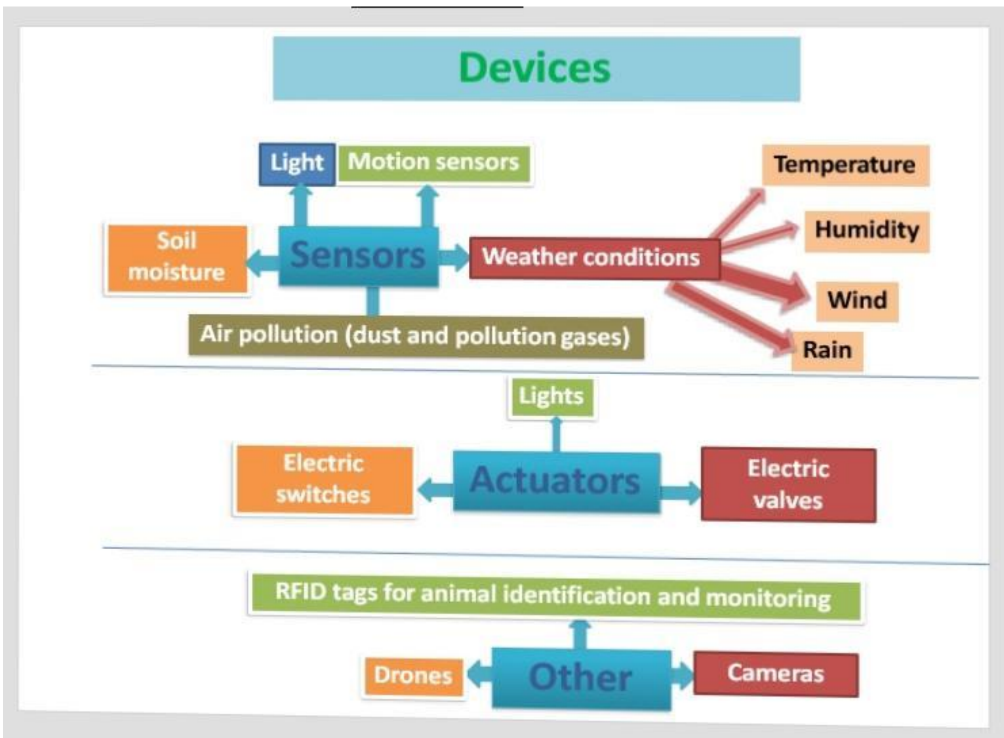
- a video analytics sensor computes traffic events based on a video feed and only pushes events (the car count, or metadata, not the individual images) through the network.
- These events go through the architectural layers and reach the applications that can drive traffic services.
- These services include traffic light coordination and also license plate identification for toll roads. Some sensors can also recognize abnormal patterns, such as vehicles moving in the wrong direction or a reserved lane.
- In that case, the video feed itself may be uploaded to traffic enforcement agencies.
- Other types of sensors that are part of traffic control solutions include Bluetooth vehicle counters, real time speed and vehicle counters, and lighting control systems.
- These sensors provide a real-time perspective while also offering data collection services for historical data trending and correlation purposes.
- Communication techniques are as varied as sensor form factors.

Smart Agriculture

Following section describes two applications viz., smart irrigation in crop fields and smart wine quality enhancing.

Smart Irrigation:

Smart irrigation deploys sensors for moisture. A smart irrigation monitoring service does the following tasks:



- Sensors for moisture and actuators for watering channels are used in smart irrigation.
- Uses soil moisture sensors with a sensor circuitry board with each one installed at certain depth in the fields.
- Uses an array of actuators (solenoid valves) which are placed along the water channels and that control deficiencies in moisture levels above thresholds during a given crop period.
- Uses sensors placed at three depths for monitoring of moisture in fruit plants such as grapes or mango, and monitors evapotranspiration (evaporation and transpiration).
- Measures and monitors actual absorption and irrigation water needs
- Each sensor board is in a waterproof cover and communicates to an access point using ZigBee protocol. An array of sensor circuits forms a WSN.
- Access point receives the data and transfers it to an associated gateway. Data adapts at the gateway and then communicates to a cloud platform using LPWAN.

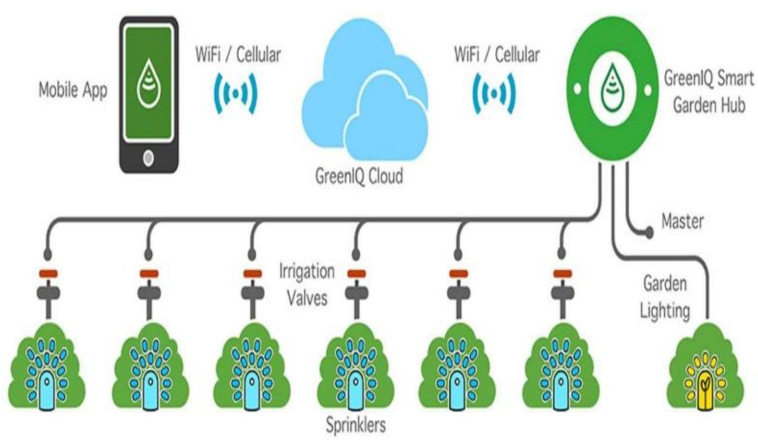
- The cloud platform may be deployed such as Nimbits, my.openHAB, AWS or Bluemix.
- Analytics at the platform analyses the moisture data and communicates to the actuators of water irrigation channels as per the water needs and past historical data
- The platform uploads the programs to sensors and actuators circuitry and sets preset measurement intervals of T1 (say, 24 hour) each and the preset actuation interval of t2 (say, on 120 hour)
- Sensed moisture values when exceed preset thresholds then trigger the alarm
- An algorithm uploads and updates the programs for the gateways and nodes.
- Runs at the data-adaptation layer and finds the faulty or inaccessible moisture
- sensors at periodic intervals
- Open source SDK and IDE are used for prototyping the monitoring system.

Impact of IOT on irrigation:

Innovations in smart irrigation have provided farmers with more effective water management tools that may help maximize efficiency and minimize overwatering.
Wireless connected sensors control water flow in fields. This saves the wastage and gets activated only when the soil gets dry. most smart irrigation technologies fall under two classifications:

- **Sensor-based control:** This method leverages real-time measurements from locally installed sensors to automatically adjust irrigation timing to the exact temperature, rainfall, humidity and soil moisture present in a given environment. This data is also supplemented with historic weather information to ensure farmers are able to anticipate unfavourable conditions.
- **Signal -based control:** Unlike sensor-based controls, these smart irrigation systems rely on weather updates transmitted by radio, telephone or web-based applications. These signals are typically sent from local weather stations to update the "evapotranspiration rate" of the irrigation controller.

GREEN IQ:



The GreenIQ system has three components.
1.Green is smart garden Hub:

- Connects to your garden’s irrigation valves.
- Optionally connects to your garden's lighting circuit.
- Controls irrigation and lighting schedules.

- Connects to the internet via WiFior cellular or Eathernet cable.

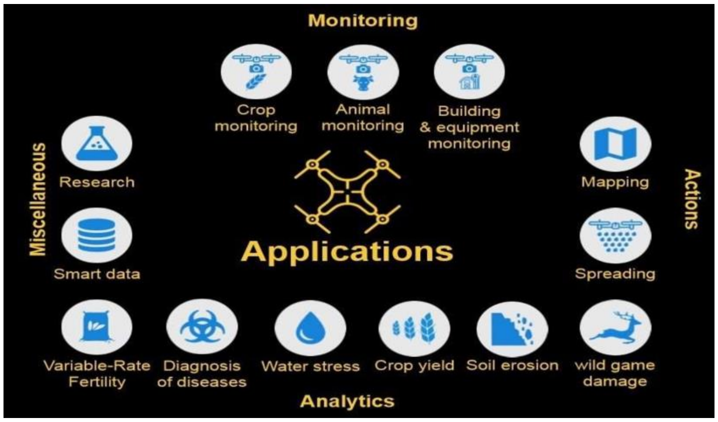
2.**Green IQ mobile app:**

- Control irrigation via smartphone or tablet with the GreenIQ app.
- The app is user-friendly and full of features and programs to easily control the entire garden.
- Water and electricity usage and savings report.
- Evapotranspiration and rainfall indicators. ...

3.Green IQ Cloud:

- All the system configurations and user programs are stored in Green IQ Cloud.
- The Green IQ smart Hub and green IQ App communicate via Green IQ Cloud.
- Configuration changes and software updates and on on-going status updates are stored and retrieved via Green IQ Cloud.

Drones in Agriculture:



Drones are currently used in two standard agricultural applications — tracking and distribution.

- Tracking (and subsequent analysis) is used in both plant and livestock agriculture and helps farmers understand the status, resources, and productivity of their farms.
- Distribution using drones involves physically moving resources across a farm, including spreading agricultural chemicals such as pesticides, fungicides, and fertilizer.

Monitoring Plant Health:

Drones equipped with special imaging equipment called Normalized Difference Vegetation Index (NDVI) use detailed colour information to indicate plant health. This allows farmers to monitor crops as they grow so any problems can be dealt with fast enough to save the plants. This image illustrates simply how NDVI works.

Monitoring Field Conditions:

Drone field monitoring is also being used to monitor the health of soil and field conditions. Drones can provide accurate field mapping including elevation information that allow growers to find any irregularities in the field. Having information on field elevation is useful in determining drainage patterns and wet/dry spots which allow for more efficient watering techniques.

Planting & Seeding:

One of the newer and less wide spread uses of drones in agriculture is for planting seeds. Automated drone seeders are mostly being used in forestry industries right now, but the potential for more widespread use is on the horizon. Planting with drones means very hard to reach areas can be replanted without endangering workers.

Spray Application:

Drone sprayers are able to navigate very hard to reach areas, such as steep tea fields at high elevations. Drone sprayers save workers from having to navigate fields with backpack sprayers, which can be hazardous to their health. Drones sprayers delivery very fine spray applications that can be targeted to specific areas to maximize efficiency and save on chemical costs.

Prerequisites for designing IoT models:

1. **Robust Models:** The characteristic features of agriculture sector such as diversity, complexity spatio-temporal variability, and uncertainties have to be considered in developing the right kinds of products and services.
2. **Scalability:** The size of farms varies from small to large, and hence the solutions should be scalable. The architecture should be able to scale up incrementally with less overheads.
3. **Affordability:** Affordability is the key to success .The cost has to be appropriate with substantial benfits. Standardized platforms, tools, products and services can bring the cost down with increased volumes.
4. **Sustainability:** The issue of sustainability is vital because of intense economic pressure and fierce global competition.

Constraints for implementing IoTin Indian agricultural scenario:

- Small, dispersed land holdings
- Complexity, scalability and affordability of the technologies.
- Privacy and security concerns
- Internet connectivity and availability
- Low awareness of IoT devices and systems among consumers
- Lack of investment and venture capital funds
- Environmental impact
- Influences human moral decision making.

Applications of IoT in agriculture:

- Monitoring soil moisture and temperature controlled irrigation
- Efficient usage of inputs like water, fertilizers, pesticides, etc.
- Reduced cost of production
- Connected greenhouses and stables
- Livestock monitoring
- Pest monitoring
- Storage monitoring
- Tracking farm products
- Prevention of illegal logging
- Mobile money transfer
- Connected cows to monitoring the feeding and breeding of animals through RFID sensors.
- Connected tractor.

Public Safety

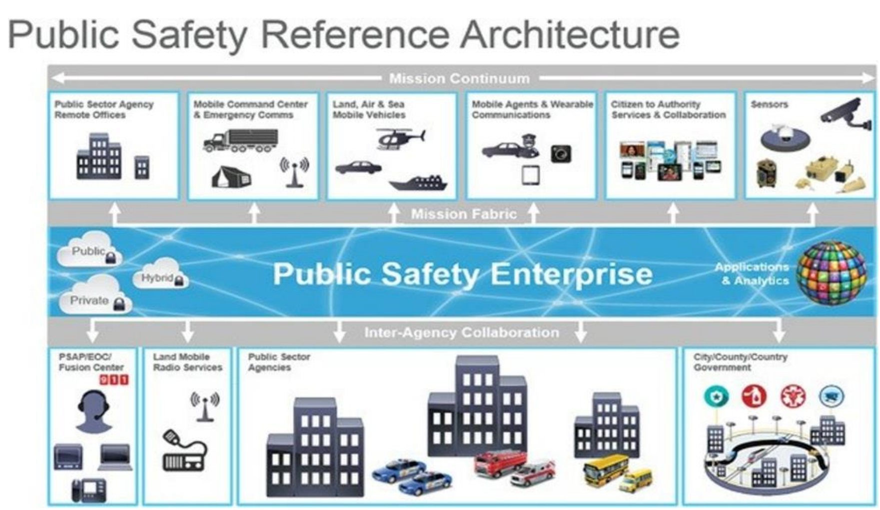
- **Public safety,** includes the different objects, vehicles, and services that interact to allow for an efficient emergency response.
- **An IoT Blueprint for Public Safety:** Explains the concept of mission continuum and lists the various elements needed to ensure the public safety mission.
- **Emergency Response IoT Architecture:** This section details the IoT and communication architectures needed for various emergency response vehicles, including the command center and mobile field vehicles.
- **IoT Public Safety Information Processing:** This section provides an overview of how big data and information processing improve emergency response efficiency.
- **School Bus Safety:** This section expands public safety applications to school buses to show how connected public vehicles can improve public services and safety.

New Possibilities:

IoT is opening new possibilities for connecting agencies and enhancing situational awareness and response capabilities across the mission environment, helping provide the following:

- Real-time situational awareness
- Intra-agency communication and collaboration (for example, voice, data, video)
- Data analytics and information sharing
- Increased community engagement and stakeholder outreach

An IoT Blueprint for Public Safety:



- A consequence of the rapid technology adoption and the multiplicity of data sources and processing logics is that IoT for public services cannot be limited to a strict set of use cases.
- Designing for IoT in the public safety space implies grouping objects and data types into actionable categories. Each use case and each environment may have a unique architecture.

- IoT for public safety needs a general framework. The IoT blueprint shown in Figure provides a framework for the public safety enterprise. This framework is extensible to describe an IoT framework for almost any public safety agency, large or small. By using this blueprint as a guide, you can correlate and align new objects, applications of IoT, or requirements with the overall design.

Mission Continuum:

- **Remote offices and fixed sites:** These are fixed locations, such as a police station, a fire station, a vehicle depot, a school building, or an administrative building that supports the mission. This is where traditional networking solutions for routing, switching, unified collaboration, security, and applications are found. These networks transport IT and OT data.
- **Mobile command center and emergency communications sites:** These are temporary locations that need to be deployable, sometimes rapidly, to provide support for incident command, specialized teams, or similar functions integral to the public safety mission. IT and OT communication for these sites can be supported by kit-based or specially designed vehicle-mounted solutions for connectivity and operation. These sites may locally process data collected from the field and/or interact with the rest of the continuum to allow for a collective situational awareness.
- **Land, air, and sea mobile vehicles:** These mobile vehicle platforms require connectivity in motion. Examples are cars, trucks, buses, boats, and aircraft that support the public safety mission. These vehicles are typically equipped with multiple sensors and smart objects, such as cameras, tablets, and specialized devices. Technologies for these vehicles are designed to deal with harsh environments in which temperature, shock and vibration, and humidity can range widely. These locations also apply special attention to size, weight, and power (SWaP) requirements, which can be highly constrained.
- **Mobile agents and wearable communications:** These locations are the field agents themselves, or their immediate environment, typically forming a personal area network (PAN). Communication solutions for these locations are handheld or wearable solutions. The previously mentioned constraints for minimized SWaP requirements are increased here to avoid burdening the individual who carries the equipment.
- Citizen-to-authority services and collaboration: This is the interface where public safety and the public collaborate through a citizen-to-authority exchange. A common exchange is 911 emergency dialing and texting. Many other examples exist and are changing, allowing this exchange to be more robust, supporting rich media voice, video, and data in real-time interactions.
- **Sensors:** These are devices and things that collect information for the public safety mission. The possibilities in this category are expanding. The sensors can be static or mobile, located in the environment external to the public safety mission team, or integrated with the team equipment. The result is a sensor grid capable of collecting information that can be combined with applications, reporting, and analytics to drive situational awareness.

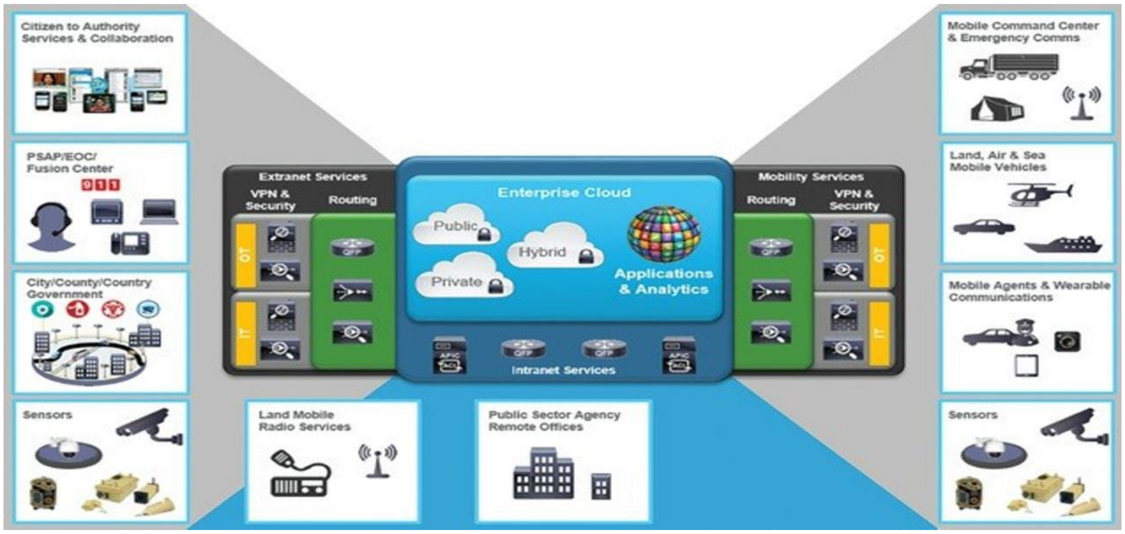
Mission Fabric:

- Within the public safety enterprise, the mission continuum and the various platforms are interconnected by the mission fabric. The mission fabric is a dynamic and flexible concept that enables fixed and mobile platforms to remain connected. It provides a uniform seamless method of enabling the various people, processes, and things to share a common set of security policies and to access applications and resources, and it is agnostic to the physical layer transport:
- Security policies are important and may vary depending on the physical or logical environment of each platform. For example, in a fixed site, the physical security of these locations should be well defined and should reduce the risk of unauthorized physical access and exposure.
- Access to applications and resources should also be seamless across the continuum, allowing personnel anywhere in the mission to perform their duties. This ability may change as bandwidth and network availability change, but it should not exclude or prevent a uniform and continuous ability to collaborate through voice, video, and data applications.
- Any physical layer transport should be compatible with the mission fabric to ensure that no matter where the mission must operate, connectivity is available. This means that any modern wired or wireless technology can be supported: Ethernet, serial, SONET and DWDM fiber optics, MPLS, Wi-Fi, commercial or private cellular, point-to-point and multipoint microwave, mobile ad hoc networking, and satellite.
- The mission fabric is the internetworking of connectivity that ties the mission continuum together into the public safety enterprise. The mission fabric must provide a seamless integration that is independent of the location characteristics (fixed or mobile platform). The mission fabric also ensures that access to resources in the cloud is uniform and agnostic to cloud type (public, private, or hybrid). In any of these configurations, the applications should have the same level of accessibility to the end users.

Inter-agency Collaboration:

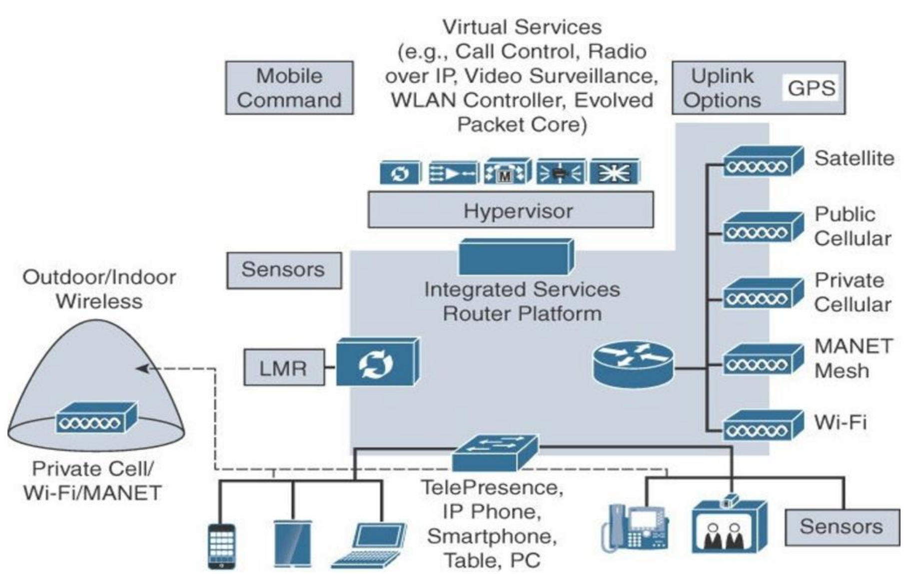
- The top half of the IoT blueprint for public safety is related to internal agency and citizen-to-authority collaboration. The lower half of the blueprint addresses inter-agency interaction as shown in above figure.
- This follows the concepts mentioned earlier about the public–private partnership. Many countries have various public safety agencies, such as PSAPs (public safety answering points, where emergency calls are answered), EOCs (emergency operations centers, where representatives from one or more agencies meet to coordinate their response to emergencies), fusion centers (typically intelligence centers that collect, analyze, and disseminate information to local agencies), and LMRS (land mobile radio services, which manage mission- critical voice communications across one or more local agencies).
- These critical elements of the public safety infrastructure are a common point of coordination and collaboration between public and private organizations.

Emergency Response IoT Architecture:



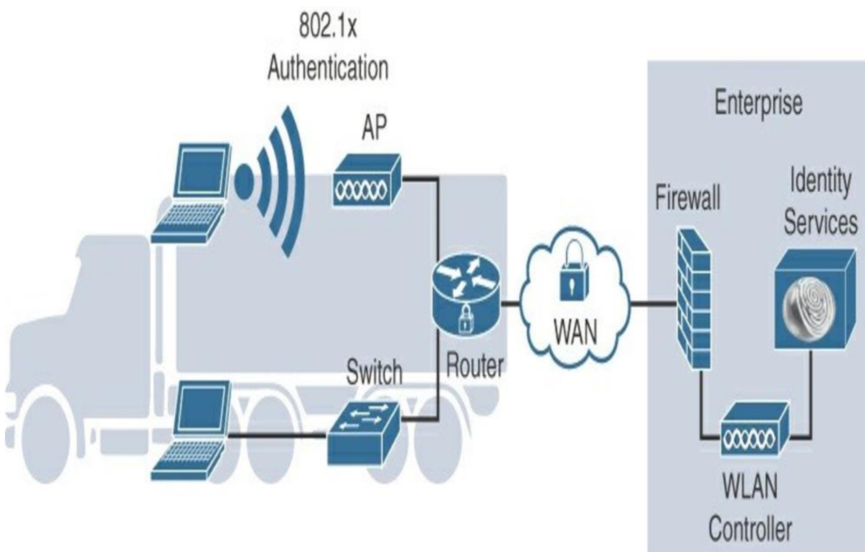
- IoT enables emergency responders to be more responsive in fulfilling their mission: protect and preserve life, property, and evidence. IoT also helps protect emergency response providers.
- Emergency responders (police officers, firefighters, and EMS personnel) operate in a very peculiar environment. Unlike workers in most other professions, emergency responders operate in unpredictable environments.
- They cannot work independently. They must collaborate with other responders, their chain of command, and the public to perform their duty successfully. The emergency response solutions needs variety of IoT capabilities available to support public agency missions.

Mobile Command Center:



- The mobile command center is an extension of the fixed office. The mobile command center serves as a communication hub during emergency situations, such as bomb threats, demonstrations, fires, or natural disasters, and it can also be used to conduct strategy meetings and other tactical operations.
- It is designed to provide a mobile office environment similar to the environment found in the agency's fixed office locations. The primary difference is that the command center can operate completely independently of the enterprise or be a fully capable remote office. Most mobile command centers operate in two possible states.
- In the first state, they move to an area of interest, and their communication systems are very limited as they move. Once onsite, they run through a brief setup process that may include activating communications systems, deploying a mast with antennas and sensors, and extending compartments that create more internal work space.
- The command center is then in the second state, and fully operational. When the mission is completed, this process is reversed to allow the vehicle to move. This method of operation is referred to as communication "on-the-pause" because the vehicle must stop before becoming operational.

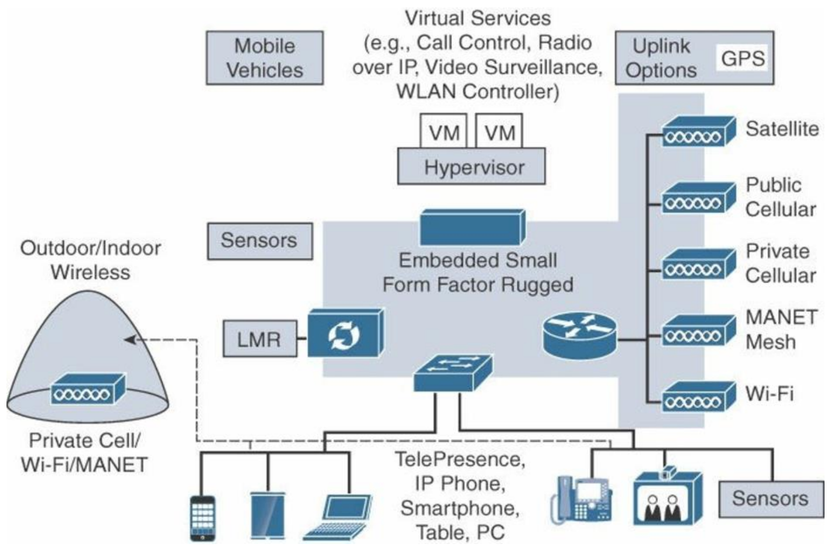
Wi-Fi communication Architecture:



- The above Figure provides a sample use case. A mobile command center does not have the same physical security protections as a fixed office. Any individual in range of the command center can detect the Wi-Fi network and attempt to eavesdrop or hijack or disrupt communications. A common deployment model uses a WLAN controller-based architecture, where the AP is in the command center, but the WLAN controller stays in the static office.
- The AP connects to the WLAN controller over the WAN uplink. User authentication occurs through the central WLAN controller and a RADIUS server. Any port on the switch in the command center is also protected with 802.1x authentication.

- If an access request cannot be authenticated, policies on the local switch or Wi-Fi access
- point can prevent access completely or limit access until authentication can be provided.
- This approach ensures that access to wired and wireless connections is managed uniformly and mitigates threats based on physical access to the vehicle.
- While access points in the vehicle are configured to provide local service, the centralized management approach offers greater security and consistency (with the central team managing all deployed wireless systems and the local team focusing on the mission).
- This ensures that a common set of security policies and access designs are available across the public safety enterprise.
- It can also reduce end-user training requirements if the Wi-Fi infrastructure in the mobile command center is consistent with that of the fixed office environment.

Land, Air, and Sea Mobile Vehicles:



- This architecture is similar to the mobile command center from the previous section but with several important distinctions.
- The most important distinction is that the mobile command center architecture is based on the concept of communications on the pause, or when the vehicle is parked.
- A mobile command center also can operate autonomously from the enterprise network and cloud services.The land, air, and sea mobile vehicles architecture is designed for communications on the move and also acts as an extension of the public safety enterprise; therefore, it is typically dependent on enterprise services such as applications.
- These platforms do not use wired uplink communications. They depend on wireless uplinks and peer connections as the vehicles are in motion on land, in the air, and a float.
- Another important distinction is the physical and environmental characteristics of mobile vehicles. Physically, the IoT solutions inside these vehicles are required to be self-contained, or at least provide a minimum equipment footprint. These vehicles are designed for mission objectives.

- For example, a fire truck or EMS vehicle has many compartments for specialized equipment. The space allocated for communications, sensors or data processing units has to be as small as possible. Environmentally, these vehicles operate at high and low temperatures, experience shock and vibration, and are exposed to humidity, moisture, and dust.
- While general-purpose equipment can be used in these vehicles, the environmental conditions can greatly reduce the life of electronic equipment. Some specialized vehicles,such as aircraft or marine vessels, may mandate equipment certified for airworthiness or for use in harsh conditions