UNIT V CASE STUDIES AND REAL-WORLD APPLICATIONS

Real-world design constraints - Applications - Asset management, Industrial automation, smart grid, Commercial building automation, Smart cities - participatory sensing - Data Analytics for IoT – Software & Management Tools for IoT Cloud Storage Models & Communication APIs – Cloud for IoT - Amazon Web Services for IoT.

Real-world design constraints in building IoT from M2M:

Devices and Networks:

- The devices that form networks in the M2M Area Network domain must be selected, or
  designed, with certain functionality suitable to IoT applications.
- The devices must have an energy source (e.g. batteries), computational capability (e.g. an
  MCU), appropriate communications interface (e.g. a Radio Frequency Integrated Circuit
  (RFIC) and front end RF circuitry), memory (program and data), and sensing (and/or actuation) capability.
- These must be integrated in such a way that the functional requirements of the desired application can be satisfied with additional nonfunctional requirements.

Functional Requirements:

- Specific sensing and actuating capabilities
- Sensing principle and data requirements: Sometimes continuous sampling of sensing data is required. For some applications, sampling after specific intervals is required.
- The parameters like higher network throughput, data loss, energy use, etc are decided based on sensing principle.

Sensing and communications field:

- The sensing field is to be considered for sensing in local area or distributed sensing. The distance between sensing points is also important factor to be considered.
- The physical environment has an implication on the communications technologies selected and the reliability of the system in operation thereafter.
- Devices must be placed in close enough proximity to communicate. Where the distance is too great, routing devices may be necessary.

Programming and embedded intelligence:

- Devices in the IoT are heterogeneous such as various computational architectures, including MCUs (8-, 16-,32-bit, ARM, 8051, RISC, Intel, etc.), signal conditioning (e.g. ADC), and memory (ROM, S/F/D) RAM, etc.), communications media, peripheral components (sensors, actuators, buttons, screens, LEDs), etc.
- In every case, an application programmer must consider the hardware selected or designed, and its capabilities.
- Application-level logic decides the sampling rate of the sensor, the local processing performed on sensor readings, the transmission schedule (or reporting rate), and the management of the communications protocol stack, among other things.
- The programmers have to reconfigure and reprogram devices in case of change in devices in IoT application.

Power:

- Power is essential for any embedded or IoT device.
- Depending on the application, power may be provided by the mains, batteries, or hybrid power sources.
- Power requirements of the application are modeled prior to deployment. This allows the designer to estimate the cost of maintenance over time.

Gateway:

- Gateway devices or proxies are selected according to need of data transitions.

Nonfunctional requirements:

The non-functional requirements are technical and non-technical.

Regulations:

- For applications that require placing nodes in public places, prior permissions are important.
- Radio Frequency (RF) regulations limit the power with which transmitters can broadcast.

Ease of use, installation, maintenance, accessibility:

- This relates to positioning, placement, site surveying, programming, and physical accessibility of devices for maintenance purposes.

Physical constraints:

- Integration of additional electronics into existing system
- Suitable packaging
- Kind and size of antenna
- Type of power supply

Financial cost:

Financial cost considerations are as follows:

- Component Selection: Typically, the use of these devices in the M2M Area Network domain is to reduce the overall cost burden. However, there are research and development costs likely to be incurred for each individual application in the IoT that requires device development or integration. Developing devices in small quantities is expensive.
- Integrated Device Design: Once the energy, sensors, actuators, computation, memory, power, connectivity, physical, and other functional and nonfunctional requirements are considered, it is likely that an integrated device must be produced.

Data representation and visualization:

Each IoT application has an optimal visual representation of the data and the system. Data that is generated from heterogeneous systems has heterogeneous visualization requirements. There are currently no satisfactory standard data representation and storage methods that satisfy all of the potential IoT applications.

IoT asset management:

IoT-based smart asset management is a step up from the traditional. These new-age smart solutions transform workflows and processes into an integrated one, building a ‘single strategic system.’ It adds intelligence with real-time data analysis, alerts, dynamic edge control of assets, predictive maintenance, and real-time asset management visibility along with automated workflows. Here are some of the key trends in IoT based

1. **Remote Asset Tracking:** IoT uses cloud-based technology, helping employees to retrieve information on the various assets anytime, anywhere.
2. **Asset Health/Condition Monitoring:** Cost-efficient and proactive method to evaluate the various health indicators and associated risks, events, policy execution history, and recommendations for improved asset health.
3. **Asset Lifecycle Management:** Comprehensive record of asset portfolio optimizing the profit generated by the various assets throughout their lifecycle.
4. **Asset Workflow Automation:** Taking care of mundane and monotonous work to accelerate business processes, reduce errors, and increase team productivity through powerful automation capabilities.
5. **Predictive Asset Maintenance**: Stay alert of your asset shutdowns and downtime by understanding the performance threshold and planning backup measures accordingly.

IoT Applications:

IoT applications promise to bring immense value into our lives. With newer wireless networks, superior sensors and revolutionary computing capabilities, the Internet of Things could be the next frontier in the race for its share of the wallet. IoT applications are expected to equip billions of everyday objects with connectivity and intelligence. It is already being deployed extensively, few applications of IoT:

- Wearables
- Smart Home Applications
- Smart Buildings
- Smart Infrastructure
- Securities
- Health Care
- Smart Cities
- Agriculture
- Industrial Automation

Industrial automation:

Industrial automation's main aim is to reduce the necessity of people in manufacturing processes. This allows production to speed up, increase in safety, and better utilize their resources and industrial analytics in manufacturing.

Impact of IoT in Industrial automation:

The Internet of Things (IoT) is a key driving factor in enabling the development of industrial automation systems. IoT coupled with computer automation controls helps streamline industrial systems and improve data automation, with the aim of removing errors and inefficiencies, primarily from the people. To achieve this at the industrial level, several layers of devices are used. IoT devices from the field (plant floor), analyzers, actuators, robotics, etc.

communicate data upwards to local process control units, which in turn send data to top-level Supervisory Control and Data Acquisition (SCADA) software. While field level machines may perform tasks automatically, at every level a human monitor can step in and interface with the system (provided they have access).

Advantages of IoT Automation:

Ability to Scale Production — Scale in production is achieved by increasing output and becoming more efficient, two objectives the digital industrial transformation enables and accelerates. It's unfortunate for workforces that the human component is sometimes the weakest link in production processes. However, by removing people from a process, companies can multiply their throughput by putting production in the hands of robots.
Increased System Uptime — Much like scale of production is limited by the human component, so too is uptime. People need rest, food, a safe working environment, and to be treated ethically. Machines on the other hand are not limited by breaks and hunger. It must be mentioned that many factory floors are very safe because automation practices can improve plant safety.
Operational Efficiency — Operational efficiency is a key business benefit that directly improves due to automation investments. This means more than using machines to perform mundane repetitive tasks, it means interconnecting systems and integrating systems to share information and allow for exponential operational improvements. With computer logic, systems can respond to other system needs. This basic application is everywhere now, from turning lights off when unneeded, to immediately informing supplier's systems around the globe that the factory system will exhaust its raw materials soon, and request a resupply.
Improved Safety for Workers — Though automation may reduce the number of line workers which can improve worker safety by minimizing the body count, using data analysis and IoT, the same automation can also improve immediate worker safety. Sensor information can be collected and analyzed to detect impending machine failures and alert maintenance staff.
Improved Regulatory Compliance — Certain companies are pressured to maintain a certain standard quality regulated by the government in their productions, which automation can help with due to its unwavering productive capabilities. This ability to eliminate, for the most part, defects in productivity allows companies to adhere to stringent regulations. For instance, in cases like food producers, the FDA Food Safety Modernization Act mandates authorities to protect consumers and promote public health, through many programs like the Current Good Manufacturing Practices (CGMP), HACCP, the FDA Retail Food Code.
Strengthened Security Access and Control through Technology — While IoT technology may introduce many attack vectors to automation systems, it also presents the solution. Physically, IoT automation can detect the presences of unauthorized individuals and alert authorities, automatically locking doors, or preventing access altogether. Advanced computer security can also take advantage of automation to defend against cyber attackers. Automation helps defenders make visible their entire network, adhere to a policy-based approach to system configuration, management, and security, and conduct many of the low-level maintenance tasks automatically while alerting IT teams of more serious breaches, or patterns that may signal attacks.

Disadvantages of IoT Automation:
Greater Connectivity Increases Attack Vectors — Unfortunately, adding more devices means more vectors for cyber attackers. IoT security is a branch of security practices that aims to solve this growing concern.
Internet Dependency — IoT and automation are heavily dependent on the Internet to function.

Redundant connectivity systems are advisable, whereas losing connectivity even for a short while could seriously cripple production with huge costs.
Complexity Increases Failure Points — Akin to more connected devices as attack vectors, the same is true for local and system failures. As the IoT automation systems grow in complexity, the weight of the inherent risk of failed components within the system must be addressed. There are many practices and designs that help overcome, including dividing the system up and adding redundancies.
IoT Planning, Building, Management Complexities — Simply, there is significant planning, building, and management of the complexities in IoT automated systems. For all their advantages, engineers must still be actively involved in these systems to ensure they continue to operate as intended.

Applications of IoT Automation:

Amazon.com — The book seller turned online marketplace, turned streaming platform, is not new to courting innovative technology. As far as logistics, Amazon has leveraged Kiva's technology in their workflows through acquisition of the company. Utilizing thousands of these Wi-Fi connected robots to fetch products, rather than humans, saves the company 20% in operating costs.
Caterpillar — The heavy machinery producer uses augmented reality technology to predict when maintenance is needed before it is absolutely needed. The application gives maintenance workers a holistic, at-a-glance view, based entirely on sensor data that maps everything from fuel levels to when filters need replacing. When replacing a filter, maintenance instructions can be sent to an AR app providing workers with all necessary information they need.
Rolls-Royce — Popularly known for their automobiles and engines, Rolls-Royce has a higher vision of replacing human-controlled cargo vessels with drone ships remotely controlled. These ships, monitored using AR technology, could manage hundreds of drone ships on the oceans that automatically navigate to their destinations using AI and machine learning. Professionals can remotely step into the driver seat when issues arise and take control of the drone ships.

Smart Grid:

The smart grid is proposed to solve the issues of electricity grid (e.g., low reliability, high outages, high greenhouse gas and carbon emission, economics, safety, and energy security). One of the definitions for the smart grid is that the smart grid is a communication network on top of the electricity grid to gather and analyze data from different components of a power grid to predict power supply and demand which can be used for power management.

Some of the required functionalities to deploy the smart grid are as follows:
1. Communication networks: Public, private, wired, and wireless communication networks that can be used as the communication infrastructure for smart grid.
2. Cybersecurity: Determining measures to guarantee availability, integrity, and confidentiality of the communication and control systems which are required to manage, operate, and protect smart grid infrastructures.
3. Distributed energy resources: Using different kinds of generation (e.g., renewable energies) and/or storage systems (batteries, plug-in electric cars with bi-directional chargers) that are connected to distributed systems.
4. Distribution grid management: Trying to maximize the performance of components in distribution systems such as feeders and transformers and integrate them with transmission systems, increase reliability, increase the distribution system efficiency, and improve

management of distributed renewable energy sources.
5. Electric transportation: Integrating plug-in electric vehicles in a large-scale.
6. Energy efficiency: Providing mechanisms for different kinds of customers to modify their energy usage during peak hours and optimizing the balance between power supply and demand.
7. Energy storage: Using direct or indirect energy storage technologies such as pumped hydroelectric storage technology.
8. Wide-area monitoring: Monitoring of power system components over a large geographic area to optimize their performance and preventing problems before they happen.
9. Advanced metering infrastructure (AMI): AMI as one of the key components of SG creates a bidirectional communication network between smart meters (SMs) and utility system to collect, send, and analyze consumer energy consumption data.

IoT Building Automation:
A Building Automation System (BAS), (also referred to as a Building Management System or a Building Control System), is a system that controls various electric, electronic and mechanical systems throughout a building.

It is a distributed control system that integrates different types of building systems together into one centralized location. Building automation systems are primarily utilized to control the heating, ventilation, and air conditioning (HVAC) in a building, but are also used to control lighting, security and other building systems.

BAS works as a computer networking system that monitors and controls a range of other electronic and mechanical systems. It provides a means for these disparate systems to communicate across platforms, software and languages.

Applications:
An extensive BAS can control many systems (such as fire and flood safety, ventilation and security) at one time, which diminishes the opportunity for human error.
A BAS system can monitor the performance of various systems.
A building automation system can provide fail-safe mechanisms to come online when electronic or mechanical failures occur. This is especially important in dangerous, high-risk work environments.
It can improve the efficiency of the other systems within a building.
An energy management system can reduce energy consumption and subsequently the operating expenses of the various systems involved.
It can extend the life cycle of various utilities so that you get more bang for your buck and less frequent repairs.
A BAS can provide a consistent level of comfort for occupants.
A building automation system can run lockouts, which ensure that machinery doesn’t turn on unless it’s supposed to.
It can run diagnostics to monitor temperature, pressures, flows, etc. over various systems.
A well-integrated BAS eliminates the redundancy that can occur when too much of the automation in a building overlaps.

Smart cities:
IoT-enabled smart city use cases span multiple areas: from contributing to a healthier environment and improving traffic to enhancing public safety and optimizing street lighting. Below, we provide an overview of the most popular use cases that are already implemented in smart cities across the globe.

Road traffic

Smart cities ensure that their citizens get from point A to point B as safely and efficiently as possible. To achieve this, municipalities turn to IoT development and implement smart traffic solutions.

Smart traffic solutions use different types of sensors, as well as fetch GPS data from drivers' smart phones to determine the number, location and the speed of vehicles. At the same time, smart traffic lights connected to a cloud management platform allow monitoring green light timings and automatically alter the lights based on current traffic situation to prevent congestion. Additionally, using historical data, smart solutions for traffic management can predict where the traffic could go and take measures to prevent potential congestion.

For example, being one of the most traffic-affected cities in the world, Los Angeles has implemented a smart traffic solution to control traffic flow. Road-surface sensors and closed-circuit television cameras send real-time updates about the traffic flow to a central traffic management platform. The platform analyzes the data and notifies the platform users of congestion and traffic signal malfunctions via desktop user apps. Additionally, the city is deploying a network of smart controllers to automatically make second-by-second traffic lights adjustments, reacting to changing traffic conditions in real time.

Smart parking

With the help of GPS data from drivers' smartphones (or road-surface sensors embedded in the ground on parking spots), smart parking solutions determine whether the parking spots are occupied or available and create a real-time parking map. When the closest parking spot becomes free, drivers receive a notification and use the map on their phone to find a parking spot faster and easier instead of blindly driving around.

Public transport

The data from IoT sensors can help to reveal patterns of how citizens use transport. Public transportation operators can use this data to enhance traveling experience, achieve a higher level of safety and punctuality. To carry out a more sophisticated analysis, smart public transport solutions can combine multiple sources, such as ticket sales and traffic information.

In London, for instance, some train operators predict the loading of train passenger cars on their trips in and out of the city. They combine the data from ticket sales, movement sensors, and CCTV cameras installed along the platform. Analyzing this data, train operators can predict how each car will load up with passengers. When a train comes into a station, train operators encourage passengers to spread along the train to maximize the loading. By maximizing the capacity use, train operators avoid train delays.

Remote monitoring

IoT smart city solutions can also provide citizens with utility management services. These services allow citizens to use their smart meters to track and control their usage remotely. For instance, a householder can turn off their home central heating using a mobile phone. Additionally, if a problem (e.g., a water leakage) occurs, utilities companies can notify householders and send specialists to fix it.

Street lighting

IoT-based smart cities make maintenance and control of street lamps more straightforward and cost-effective. Equipping streetlights with sensors and connecting them to a cloud management solution helps to adapt lighting schedule to the lighting zone.

Smart lighting solutions gather data on illuminance, movement of people and vehicles, and combine it with historical and contextual data (e.g., special events, public transport schedule, time of day and year, etc.) and analyze it to improve the lighting schedule. As a result, a smart lighting solution “tells” a streetlight to dim, brighten, switch on or switch off the lights based on the outer conditions.

For instance, when pedestrians cross the road, the lights around the crossings can switch to a brighter setting; when a bus is expected to arrive at a bus stop, the streetlights around it can be automatically set brighter than those further away, etc.

Waste management

Most waste collection operators empty containers according to predefined schedules. This is not a very efficient approach since it leads to the unproductive use of waste containers and unnecessary fuel consumption by waste collecting trucks.

IoT-enabled smart city solutions help to optimize waste collecting schedules by tracking waste levels, as well as providing route optimization and operational analytics.

Each waste container gets a sensor that gathers the data about the level of the waste in a container. Once it is close to a certain threshold, the waste management solution receives a sensor record, processes it, and sends a notification to a truck driver’s mobile app. Thus, the truck driver empties a full container, avoiding emptying half-full ones.

Environment

IoT-driven smart city solutions allow tracking parameters critical for a healthy environment in order to maintain them at an optimal level. For example, to monitor water quality, a city can deploy a network of sensors across the water grid and connect them to a cloud management platform. Sensors measure pH level, the amount of dissolved oxygen and dissolved ions. If leakage occurs and the chemical composition of water changes, the cloud platform triggers an output defined by the users. For example, if a Nitrate (NO_3^-) level exceeds 1 mg/L, a water quality management solution alerts maintenance teams of contamination and automatically creates a case for field workers, who then start fixing the issue.

Another use case is monitoring air quality. For that, a network of sensors is deployed along busy roads and around plants. Sensors gather data on the amount of CO, nitrogen, and sulfur oxides, while the central cloud platform analyzes and visualizes sensor readings, so that platform users can view the map of air quality and use this data to point out areas where air pollution is critical and work out recommendations for citizens.

Public safety

For enhancing public safety, IoT-based smart city technologies offer real-time monitoring, analytics, and decision-making tools. Combining data from acoustic sensors and CCTV cameras deployed throughout the city with the data from social media feed and analyzing it, public safety solutions can predict potential crime scenes. This will allow the police to stop potential perpetrators or successfully track them.

For example, more than 90 cities across the United States use a gunshot detection solution. The solution uses connected microphones installed throughout a city. The data from microphones passes over to the cloud platform, which analyzes the sounds and detects a gunshot. The platform measures the time it took for the sound to reach the microphone and estimates the location of the gun. When the gunshot and its location are identified, cloud software alerts the police via a mobile app.

Participatory sensing:

Participatory sensing is a form of data collection that engages individuals in collecting data about themselves and their communities using digital devices.

Collective design and investigation: in this case, the participants are involved in all the phases of the project lifecycle. Participants collectively define the research objective(s) and finalize the sensors and their sampling frequencies, security policies, and data pro-cessing and management system.

Public contribution: in this case, the participants are actively involved in the data collection phase but are not part of the group that defines the research objectives and necessary infrastructure (sensors and data management infrastructure).

Personal use and reaction: these participants are individuals focused on self-discovery and improvement.

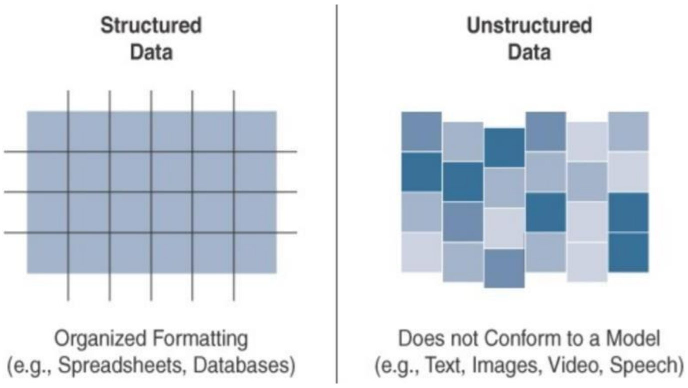
Data Analytics for IoT:

- In the world of IoT, the creation of massive amounts of data from sensors is common and one of the biggest challenges not only from a transport perspective but also from a data management standpoint. Analyzing this amount of data in the most efficient manner possible falls under the umbrella of data analytics.
- IoT data analytics is the analysis of huge data volumes generated by connected devices. Organizations can derive a number of benefits from it: optimize operations, control processes automatically, engage more customers, and empower employees.

Types of data:

Depending on how data is categorized, various data analytics tools and processing methods can be applied. Two important categorizations from an IoT perspective are whether the data is structured or unstructured and whether it is in motion or at rest.

Structured data and unstructured data are important classifications as they typically require different toolsets from a data analytics perspective. Figure 2 provides a high- level comparison of structured data and unstructured data.

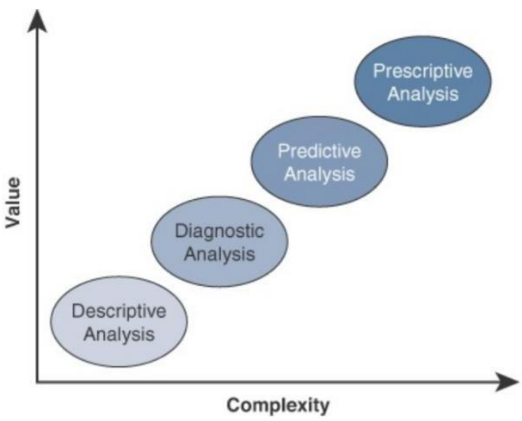


Structured data means that the data follows a model or schema that defines how the data is represented or organized, meaning it fits well with a traditional relational database management system (RDBMS).
Unstructured data lacks a logical schema for understanding and decoding the data through traditional programming means. Examples of this data type include text, speech, images, and video. As a general rule, any data that does not fit neatly into a predefined data model is classified as unstructured data. According to some estimates, around 80% of a business's data is unstructured. Because of this fact, data analytics methods that can be applied to unstructured data, such as cognitive computing and machine learning, are deservedly garnering a lot of attention.

Four types of data analysis results

Descriptive:

- Descriptive data analysis tells you what is happening, either now or in the past.
- For example, a thermometer in a truck engine reports temperature values every second.
- From a descriptive analysis perspective, you can pull this data at any moment to gain insight into the current operating condition of the truck engine.
- If the temperature value is too high, then there may be a cooling problem or the engine may be experiencing too much load.



Diagnostic:

- When you are interested in the "why," diagnostic data analysis can provide the answer.
- Continuing with the example of the temperature sensor in the truck engine, you might

wonder why the truck engine failed.
- Diagnostic analysis might show that the temperature of the engine was too high, and the engine overheated.
- Applying diagnostic analysis across the data generated by a wide range of smart objects can provide a clear picture of why a problem or an event occurred.

Predictive:
- Predictive analysis aims to foretell problems or issues before they occur.
- For example, with historical values of temperatures for the truck engine, predictive analysis could provide an estimate on the remaining life of certain components in the engine.
- These components could then be proactively replaced before failure occurs.
- Or perhaps if temperature values of the truck engine start to rise slowly over time, this could indicate the need for an oil change or some other sort of engine cooling maintenance.

Prescriptive:
- Prescriptive analysis goes a step beyond predictive and recommends solutions for upcoming problems.
- A prescriptive analysis of the temperature data from a truck engine might calculate various alternatives to cost-effectively maintain our truck
- These calculations could range from the cost necessary for more frequent oil changes and cooling maintenance to installing new cooling equipment on the engine or upgrading to a lease on a model with a more powerful engine.
- Prescriptive analysis looks at a variety of factors and makes the appropriate recommendation
- Both predictive and prescriptive analyses are more resource intensive and increase complexity, but the value they provide is much greater than the value from descriptive and diagnostic analysis

IoT Data Analytics Challenges:

Scaling problems: Due to the large number of smart objects in most IoT networks that continually send data, relational databases can grow incredibly large very quickly. This can result in performance issues that can be costly to resolve, often requiring more hardware and architecture changes.

Volatility of data: With relational databases, it is critical that the schema be designed correctly from the beginning. Changing it later can slow or stop the database from operating. Due to the lack of flexibility, revisions to the schema must be kept at a minimum. IoT data, however, is volatile in the sense that the data model is likely to change and evolve over time. A dynamic schema is often required so that data model changes can be made daily or even hourly.

Cloud for IoT:
An IoT cloud is a massive network that supports IoT devices and applications. This includes the underlying infrastructure, servers and storage, needed for real-time operations and processing. An IoT cloud also includes the services and standards necessary for connecting, managing, and securing different IoT devices and applications. IoT generate a huge amount of data or big data. Managing the flow and storage of this data is a tedious task for enterprises.

Cloud computing with its different models and implementation platforms help companies to manage and analyze this data, enhancing the overall efficiency and working of IoT system. DLM, AEP, and Digital Twins are some of the solutions better leveraged through cloud platforms like Amazon Web Services (AWS) and Microsoft Azure.

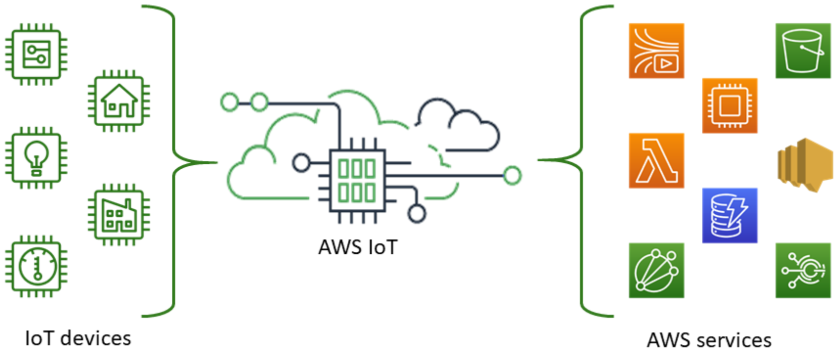
IoT Cloud Platforms:

Following are the cloud platforms including the Software & Management Tools for IoT Cloud:

1. Thingworx 8 IoT Platform
2. Microsoft Azure IoT Suite
3. Google Cloud's IoT Platform
4. IBM Watson IoT Platform
5. AWS IoT Platform
6. Cisco IoT Cloud Connect
7. Salesforce IoT Cloud
8. Kaa IoT Platform
9. Oracle IoT Platform
10. Thingspeak IoT Platform

Amazon Web Services for IoT:

AWS IoT provides the cloud services that connect your IoT devices to other devices and AWS cloud services. AWS IoT provides device software that can help you integrate your IoT devices into AWS IoT-based solutions. If your devices can connect to AWS IoT, AWS IoT can connect them to the cloud services that AWS provides.



AWS IoT lets you select the most appropriate and up-to-date technologies for your solution. To help you manage and support your IoT devices in the field, AWS IoT Core supports these protocols:

MQTT (Message Queuing and Telemetry Transport)

MQTT over WSS (Websockets Secure)

HTTPS (Hypertext Transfer Protocol - Secure)

LoRaWAN (Long Range Wide Area Network)

The AWS IoT Core message broker supports devices and clients that use MQTT and MQTT over WSS protocols to publish and subscribe to messages. It also supports devices and clients that use the HTTPS protocol to publish messages.

AWS IoT Core for LoRaWAN helps you connect and manage wireless LoRaWAN (low-power long-range Wide Area Network) devices. AWS IoT Core for LoRaWAN replaces the need for you to develop and operate a LoRaWAN Network Server (LNS).

Three key categories of IoT products on AWS:

Devices Software: It includes services such as the FreeRTOS and AWS IoT Greengrass, etc.
Connectivity & Control Services: It includes services like AWS IoT Core, AWS IoT Device Defender & AWS IoT Device Management, etc.
Analytics Services: It includes services such as AWS IoT Events, AWS IoT Analytics, AWS IoT SiteWise & AWS IoT ThingsGraph, etc.
Now let’s get an overview of each category and the IoT products associated with them.

1. Device Software
Device Software is used to connect your devices and operate them at the edge.

FreeRTOS: It is an open-source real-time operating system for embedded systems that can be used in IoT. It is suitable for programming low-power systems, their deployment, security, and connection. It is open and freely available under MIT open source license. It comes with a kernel and set of suitable libraries which we would need for different sectors. Using Amazon FreeRTOS we can connect the low power devices with the cloud’s powerful services. Free RTOS can be easily reused and has high reliability. It comes with the features like microcontrollers support, FreeRTOS console, secure connection of devices, connectivity with cloud, etc.

AWS IoT Greengrass: AWS IoT Greengrass is an open-source runtime for IoT edge devices and cloud services. It is widely used by people in homes, factories, vehicles, and businesses. We can easily build intelligent device software on IoT Greengrass. It comes with features like local processing, messaging, data management, and other Machine learning interfaces. It also allows us to remotely manage the devices. It also makes the device smarter over time by keeping it up-to-date.

2. Connectivity & Control Services
These services are used to secure, control, and manage your devices from the cloud.

AWS IoT Core: AWS IOT core enables the IoT devices to securely and easily communicate with the cloud. It can support up to billion devices easily. It can also process trillions of messages at once and send them to suitable endpoints. It mainly helps devices that use protocols like MQTT over WSS to publish their messages.

AWS IoT Device Defender: AWS IOT device defender is mainly used to secure a group of IoT devices. It is responsible for the safety of IoT devices. It enforces the safety measures such as identity, authentication, authorization of devices, and encryption of the device’s data.

AWS IoT Device Management: AWS IoT Device Management mainly helps in monitoring and tracking IoT devices. It is very much useful for the management of IoT devices. Using this we can remotely monitor the health of each device, problems with the devices, and necessary steps to be taken. The important benefit is that we can overlook the status of the fleet of devices all at once.

3. Analytics Services

The Analytics Services are used to work with IoT data faster to extract value from your data.

AWS IoT Events: As the name indicates AWS IOT Events helps the user to watch over the devices by the events or notifications it sends. Its events are sent when an error occurs or when any actions need to be triggered. Using this we can build complex monitoring services for our IoT products. The major benefits of AWS IOT events include getting inputs from multiple sources, Usage of simple logical expressions to recognize complex cases of events, Triggering actions based on the events, Automatically scaling the system to meet the IoT fleet's demands.

AWS IoT Analytics: AWS IOT Analytics mainly analyzes and scales the IoT data. It easily supports up to petabytes of IoT data. So it is highly efficient. It eliminates the need to manage complex IoT infrastructure and helps in building fast and responsive IoT applications. It can be used to operate huge volumes of IoT data without needing to worry about the infrastructure needed for its processing. Since IoT data is highly unstructured and susceptible to false readings it is necessary to preprocess and analyze it properly for accurate and better results it can be done by AWS IOT analytics.

AWS IoT SiteWise: AWS IoT Sitewise allows us to collect, model, and analyze the data from the industrial IOT devices which are at scale. We can also gain insights into industrial operations by configuring the suitable metrics using AWS IOT Sitewise. We can also effectively process the data on the local devices with IoT Sitewise Edge. Some benefits of it include, it collects the data from all the sources consistently, even identifies remote issues with quick monitoring, improving the cross-facility process with a central data source, process and monitoring the data on-premises for better shop floor applications.

AWS IoT ThingsGraph: AWS IoT Things Graph is used to connect web services and other different devices visually for building IoT applications. It provides a drag and drop interface which makes it easy for us to build IoT applications easily by connecting devices and web services quickly. Some of the benefits of the IoT things graph include allowing us to build IoT applications faster, can easily create sophisticated workflows, very easily monitoring and managing the devices.