IoT Solutions
Module-IV

Dr Shola UshaRani

IoT Levels & Deployment Templates

An IoT system comprises of the following components:

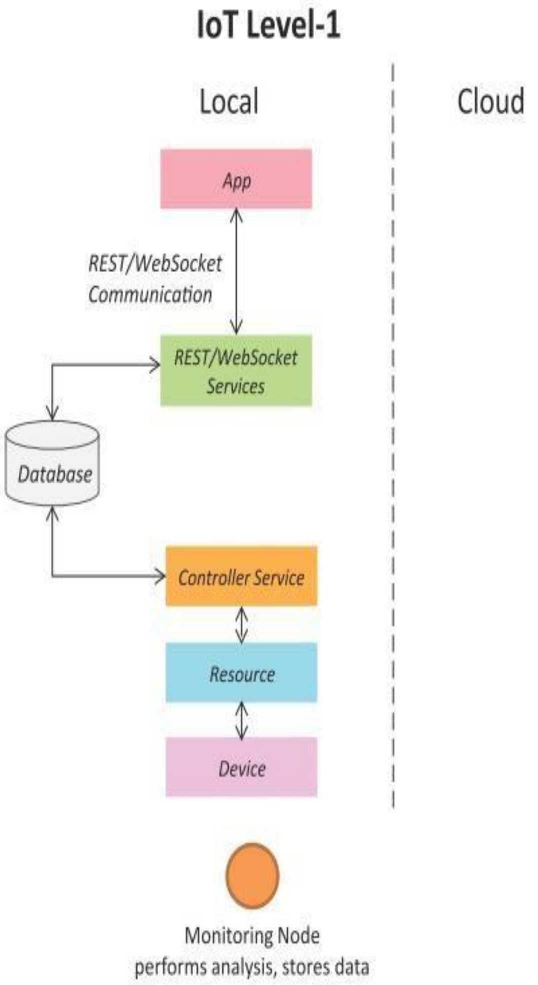
- **Device**: An IoT device allows identification, remote sensing, actuating and remote monitoring capabilities.
- **Resource**: Resources are software components on the IoT device for accessing, processing, and storing sensor information, or controlling actuators connected to the device. Resources also include the software components that enable network access for the device.
- **Controller Service**: Controller service is a native service that runs on the device and interacts with the 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.

IoT Levels & Deployment Templates

- **Database**: Database can be either local or in the cloud and stores the data generated by the IoT device.
- **Web Service**: Web services serve as a link between the IoT device, application, database and analysis components. Web service can be either implemented using HTTP and REST principles (REST service) or using WebSocket protocol (WebSocket service).
- **Analysis Component**: The Analysis Component is responsible for analyzing the IoT data and generate results in a form which are easy for the user to understand.
- **Application**: IoT applications provide an interface that the users can use to control and monitor various aspects of the IoT system. Applications also allow users to view the system status and view the processed data

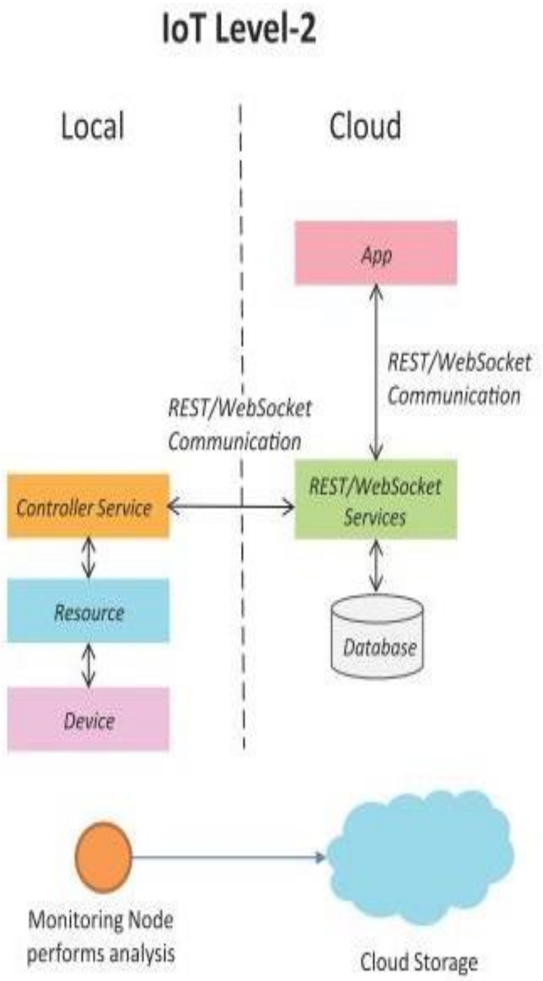
IoT Level–1

- A level–1 IoT system has a single node/device that performs sensing and/or actuation, stores data, performs analysis and hosts the application
- Level–1 IoT systems are suitable for modeling low– cost and low–complexity solutions where the data involved is not big and the analysis requirements are not computationally intensive.



IoT Level–2

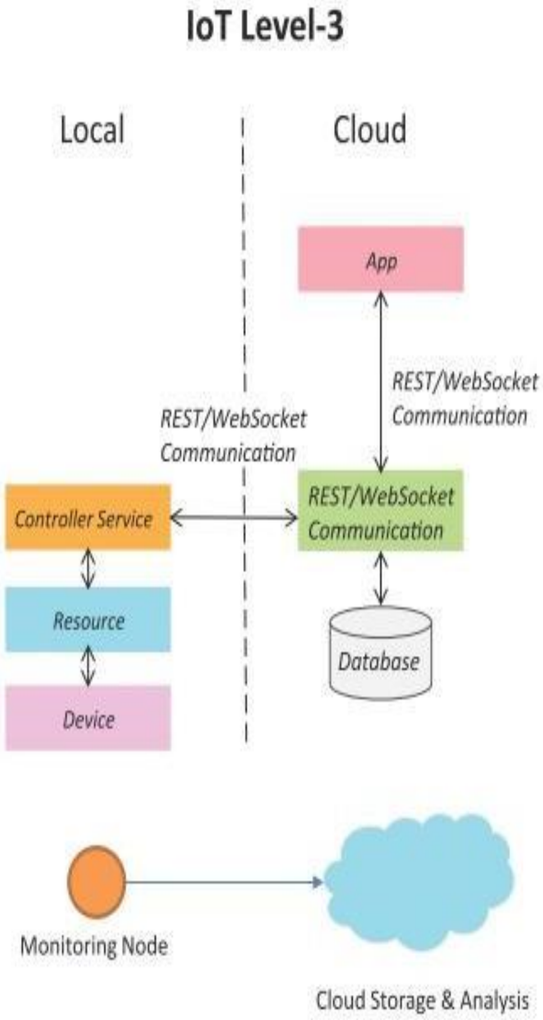
- A level–2 IoT system has a single node that performs sensing and/or actuation and local analysis.
- Data is stored in the cloud and application is usually cloud–based.
- Level–2 IoT systems are suitable for solutions where the data involved is big, however, the primary analysis requirement is not computationally intensive and can be done locally itself.



Bahga & Madisetti, ©

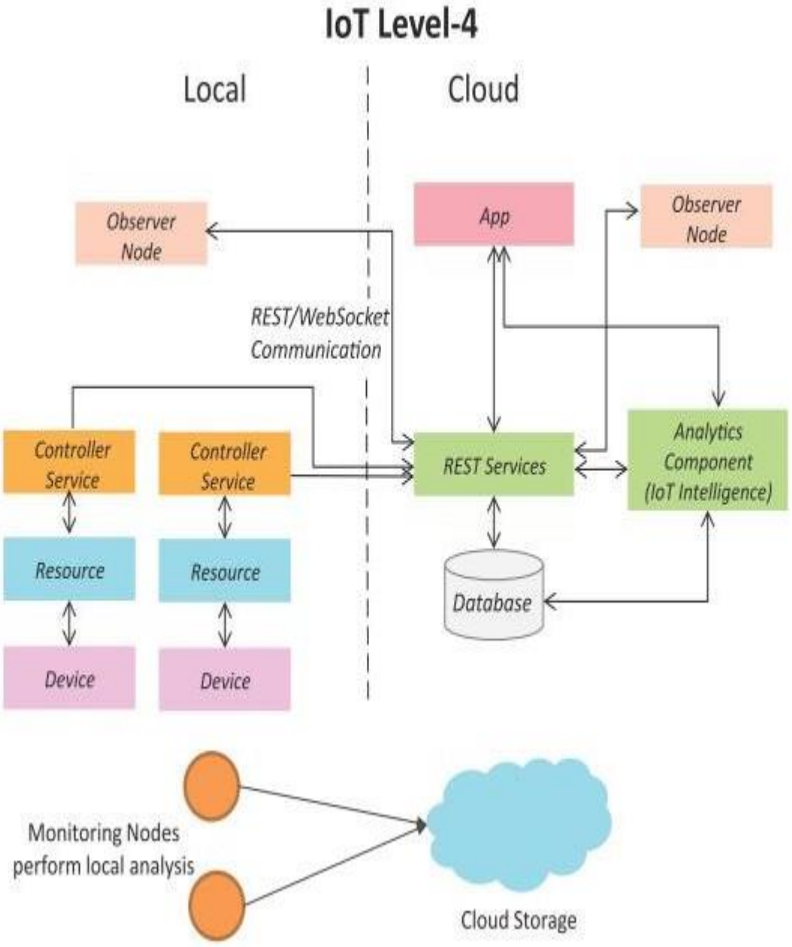
IoT Level–3

- A level–3 IoT system has a single node. Data is stored and analyzed in the cloud and application is cloud– based.
- Level–3 IoT systems are suitable for solutions where the data involved is big and the analysis requirements are computationally intensive.



IoT Level–4

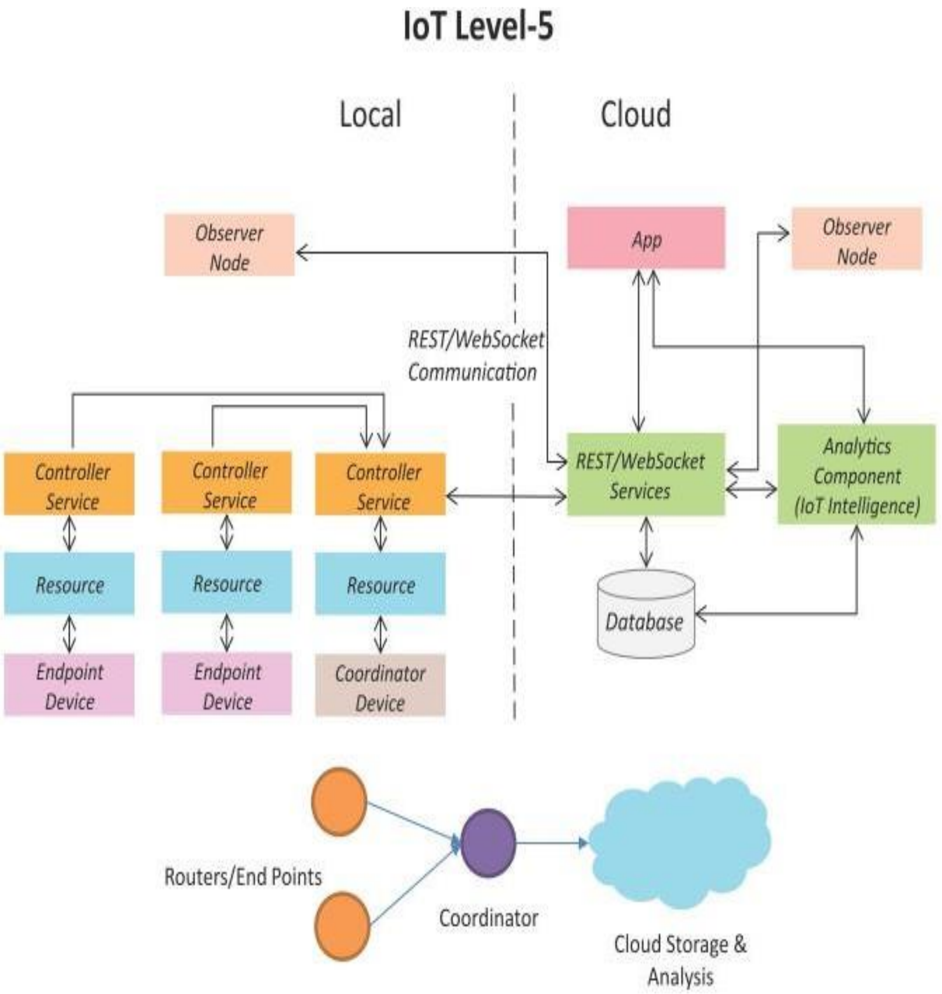
- A level–4 IoT system has multiple nodes that perform local analysis. Data is stored in the cloud and application is cloud–based.
- Level–4 contains local and cloud– based observer nodes which can subscribe to and receive information collected in the cloud from IoT devices.
- Level–4 IoT systems are suitable for solutions where multiple nodes are required, the data involved is big and the analysis requirements are computationally intensive.



Bahga & Madisetti, © 2015

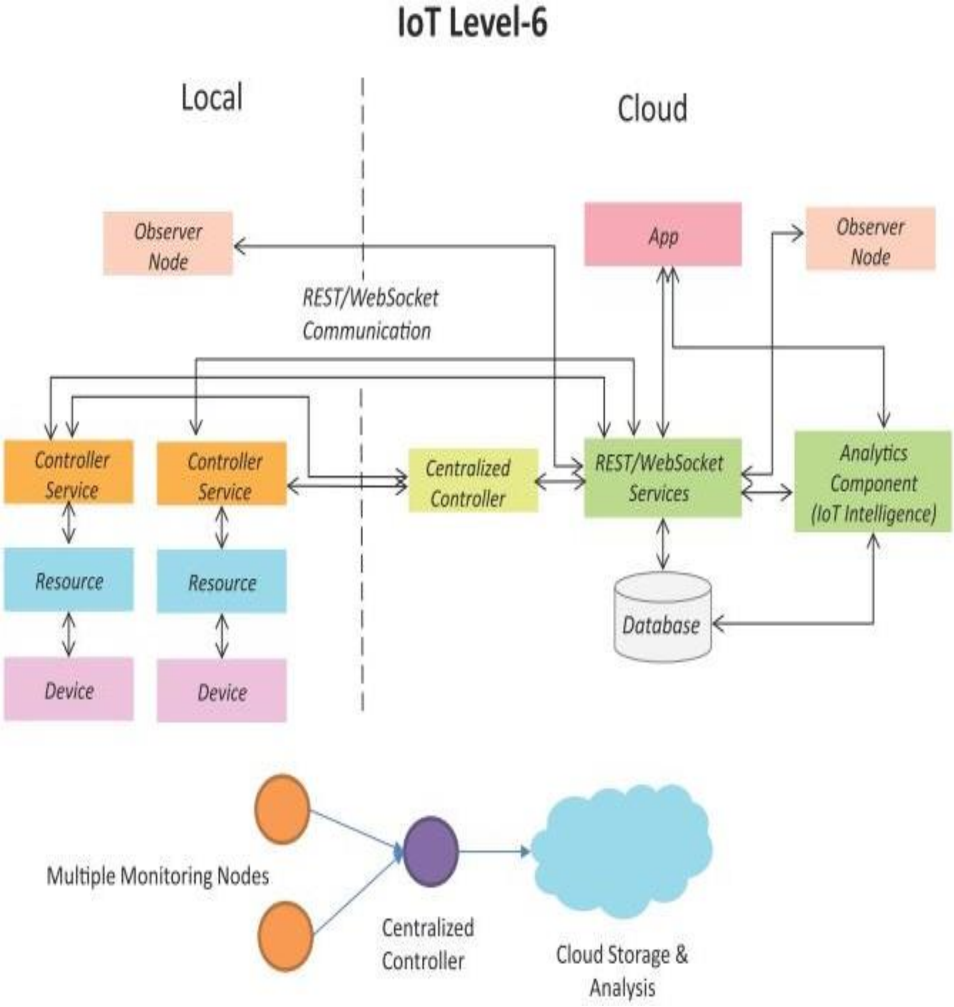
IoT Level–5

- A level–5 IoT system has multiple end nodes and one coordinator node.
- The end nodes that perform sensing and/or actuation.
- Coordinator node collects data from the end nodes and sends to the cloud.
- Data is stored and analyzed in the cloud and application is cloud–based.
- Level–5 IoT systems are suitable for solutions based on wireless sensor networks, in which the data involved is big and the analysis requirements are computationally intensive.



IoT Level–6

- A level–6 IoT system has multiple independent end nodes that perform sensing and/or actuation and send data to the cloud.
- Data is stored in the cloud and application is cloud–based.
- The analytics component analyzes the data and stores the results in the cloud database.
- The results are visualized with the cloud–based application.
- The centralized controller is aware of the status of all the end nodes and sends control commands to the nodes.



Bahga & Madisetti, ©

Examples

1. Smart home system having one device controlling all the devices stores its information locally
2. Smart irrigation system : single node monitors soil moisture levels, if the levels of the moisture below threshold values switch ON the irrigation system. The moisture data is stored in cloud using REST based web service. A cloud application is used to access the data from the cloud.
3. Tracking packaging handling : knowing about the vibration levels of the package. Used accelerometer and gyroscope sensors for measuring the vibration levels. Controller sends the data to cloud. The data can be viewed using cloud based application. Analysis component in cloud triggers the alerts the vibration levels if the thresholds are greater.

Examples-4

- Noise monitoring system : multiple nodes are kept at different places. The nodes are sound sensors which will measure the noise from sensors. Each independent node its sensed data to the local controller service. From that local to cloud. This data is stored in the data based at cloud. Observer nodes at cloud side collect it and perform some analysis. The cloud application use this analysed data for visualizing and aggregating it.

Example-5

- **Forest fire detection** : multiple nodes are kept different places of the forest. These nodes are used to monitor temperature, humidity and carbon dioxide(Co2) . All these nodes data are collected by a coordinator node called as Gateways connects the internet connectivity. This coordinator from local storage place the data into cloud. The observer node at Cloud will perform the computation on this stored data.

Example-6

- Weather monitoring system: the system consists of multiple nodes which will monitor temperature, humidity and pressure in the area. This data is communicated to cloud through observer nodes. Then observer node collects the data from cloud database and performs analytics. The aggregated data from the observer node is also used to perform the predictions

IoT Level design

- Write the problem statement of your J component and derive the IoT Level design of your problem . Justify the answer.

Nodes	IoT Level-I	IoT Level-II	IoT-Level III	IoT Level IV	IoT Level V	IoT Level VI
Monitoring Node	yes	yes	yes	yes	Yes	Yes
Observer Node				Yes	Yes	Yes
Centralised coordinator					Yes	Yes
Centralized controller						Yes
complexity	LOW					High
Cost	LOW					High

Use case development

- What it is?
- Its importance
- IoT design development steps

What is Use Case development

- Knowing about **working of project**, what to create and how to create.
- Definition
  - a list of actions or event steps, typically defining the interactions between a role (known in the Unified Modeling Language as an *actor*) and a system, to achieve a goal.
  - The actor can be human, system or time etc.,

Importance of Use Case

- It provides the shortest summary of what the system will offer.
- It gives an overview of the roles of each and every component in the system.
- It will help us in defining the role of users, administrators etc.
- It helps us in extensively defining the user’s need and exploring it as to how it will work.
- It provides solutions and answers to many questions that might pop up if we start a project unplanned.

Need for IoT solution

- IoT system is complex with various challenges
  - Provide various interactions among all the components required for network resources, web services, analytical components, applications and database services.
- Wide range of choices available to each of these components.
  - Designing the IoT system specific to produce and service choices in mind.
- Various vendors for all components : compromise to costs or design methodology
  - Cannot replace the component to add new features.

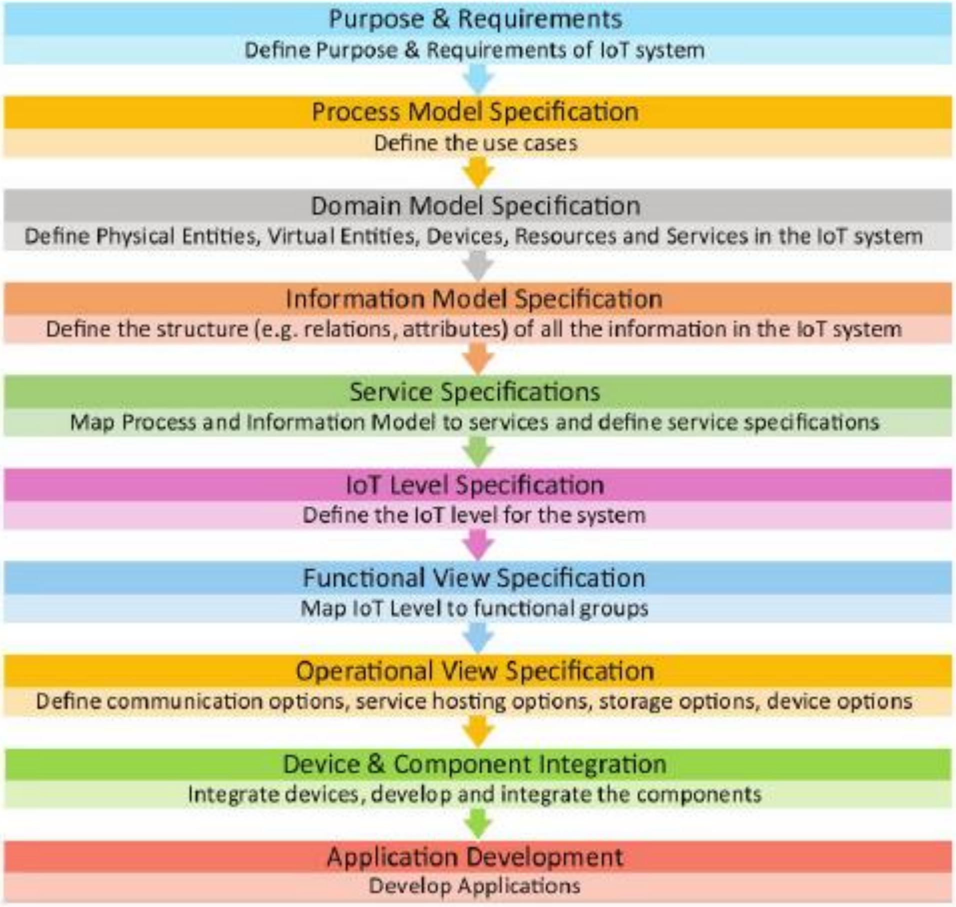
Goals of IoT solution

- To provide many interactions among various components.
- To design the System with specific products/services
- To the design IoT methodology for the system which is independent of specific product and programming language.

IoT Solution design Methodology

Steps given and explained based on home automation system.

IoT System Design Methodology



Purpose & Requirements

Define Purpose & Requirements of IoT system

Process Model Specification

Define the use cases

Domain Model Specification

Define Physical Entities, Virtual Entities, Devices, Resources and Services in the IoT system

Information Model Specification

Define the structure (e.g. relations, attributes) of all the information in the IoT system

Service Specifications

Map Process and Information Model to services and define service specifications

IoT Level Specification

Define the IoT level for the system

Functional View Specification

Map IoT Level to functional groups

Operational View Specification

Define communication options, service hosting options, storage options, device options

Device & Component Integration

Integrate devices, develop and integrate the components

Application Development

Develop Applications

Home automation system

- A home automation system, allowing and controlling of lights through an web based application. It has two types of modes Auto mode and Manual mode to control the operation of lights

Purpose & Requirements Specification

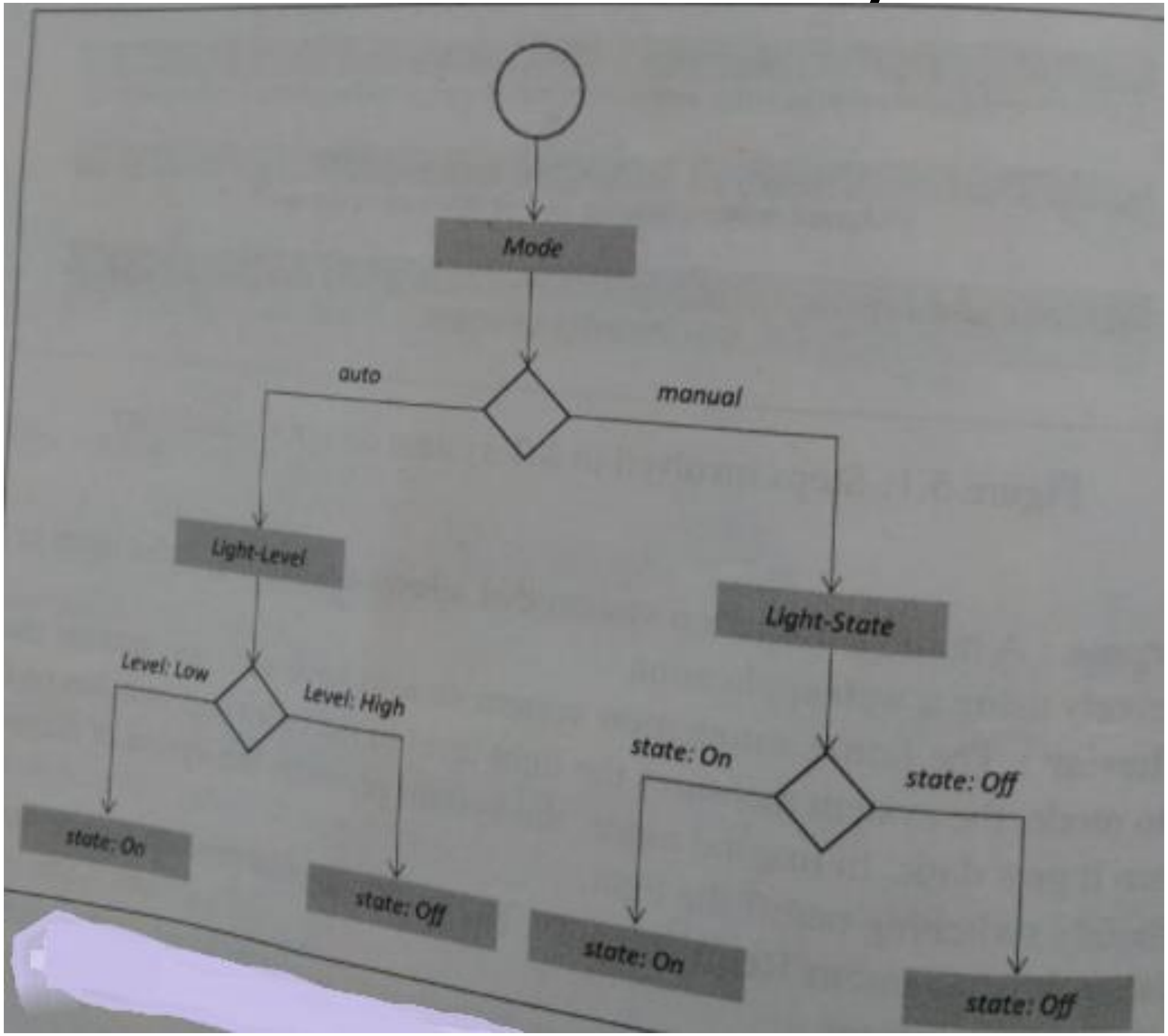
Purpose, behaviour and requirements like **data collection, data analysis, system management requirements**

- Purpose: for home automation system, allowing and controlling of lights through an web based application.
- Behaviour: two types of modes
  - Auto mode : measures the light level in the room and switches ON/OFF the light
  - Manual mode : provides option of manual or through remotely.
- System Management Requirements
  - Provision of control operations and remote monitoring.
- Data Analysis Requirement
  - Analysis of data locally.
- Application deployment requirement
  - Application is deployed locally but accessed remotely.
- Security Requirement
    - Use authentication capability.

Process Specification

- Defining the use cases based on step1
- Process representation using flow diagrams.
- Various symbols:
  - Circle : about start of the process
  - Decision box
  - Rectangle : state or attributes.

Process specification for home automation IoT system



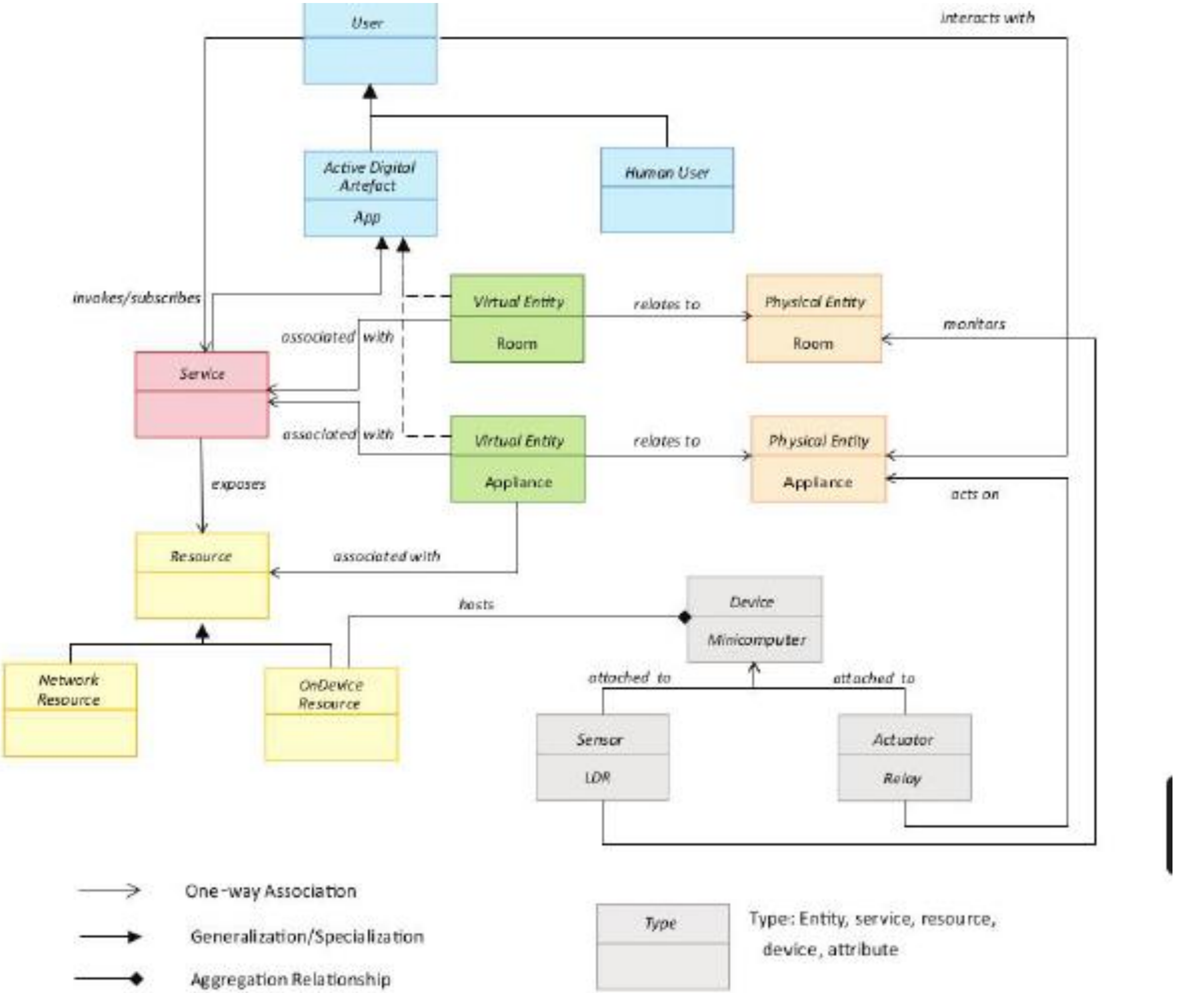
Domain Model Specification

- It represents the main concepts, entities and objects in the IoT system.
- It is independent of technology and platform.
- Defines the attributes of objects, relationship between objects
- It is an abstract representation of the concepts, objects and entities.
  - Physical Entity
  - Virtual Entity
  - Device
  - Resource
  - Service

Domain Model Specification

- Physical Entity
  - Discrete and identifiable entity of physical environment
    - Home automation system physical entities like room and light appliance.
- Virtual Entity
  - Representing the digital form of physical entity.
  - For each physical entity there was one virtual entity in the model.
  - Virtual entity for room is monitoring and for appliances is controller.
- Device
  - Interaction between physical entity and virtual entity.
  - Devices for gathering the information about physical entities
  - For home automation system mini computer is attached with light sensor and actuator.
- Resource
  - Software component information for on-devices and network resources.
    - The software for on devices will provide the information of the physical entity once it is actuated upon.
    - Similarly the software enables the network resources like databases.
  - For home automation system, the operating system is a software component that runs on the mini computer.
- Service
  - An interface for interacting with physical entity.
  - The service access the resource hosted on the device or the network resource to obtain information about the physical entity or perform actuation upon physical entity.

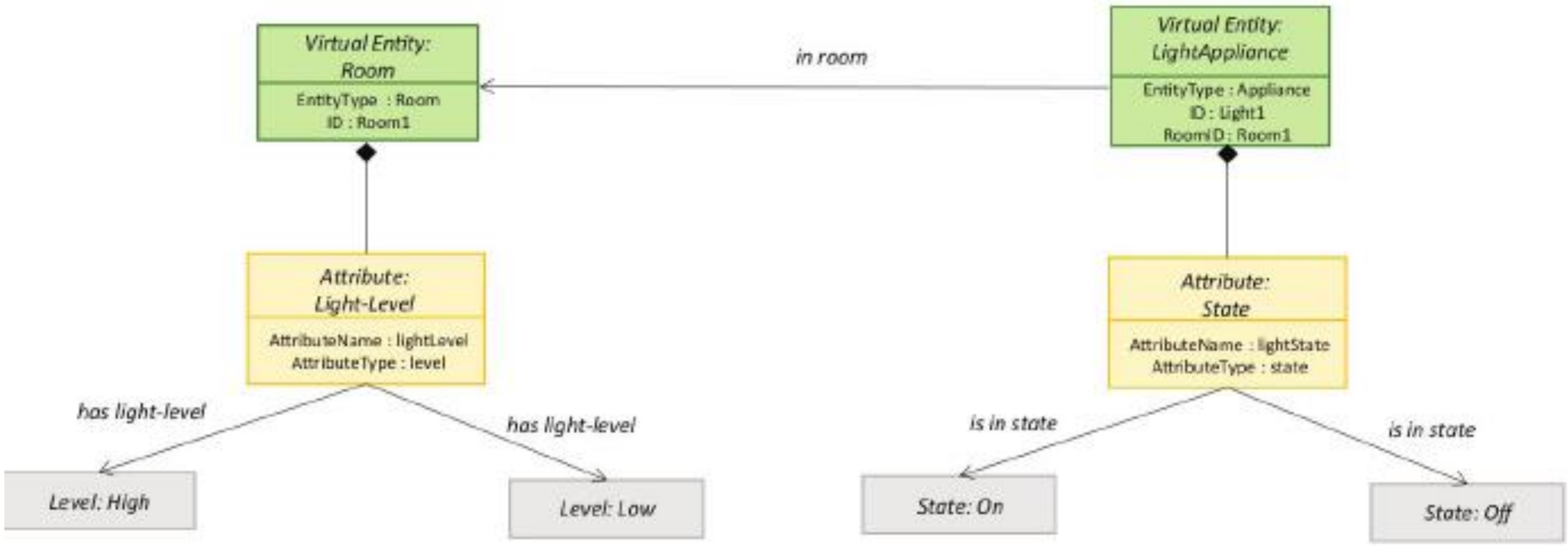
Domain Model for Home automation IoT System



Information Model Specification

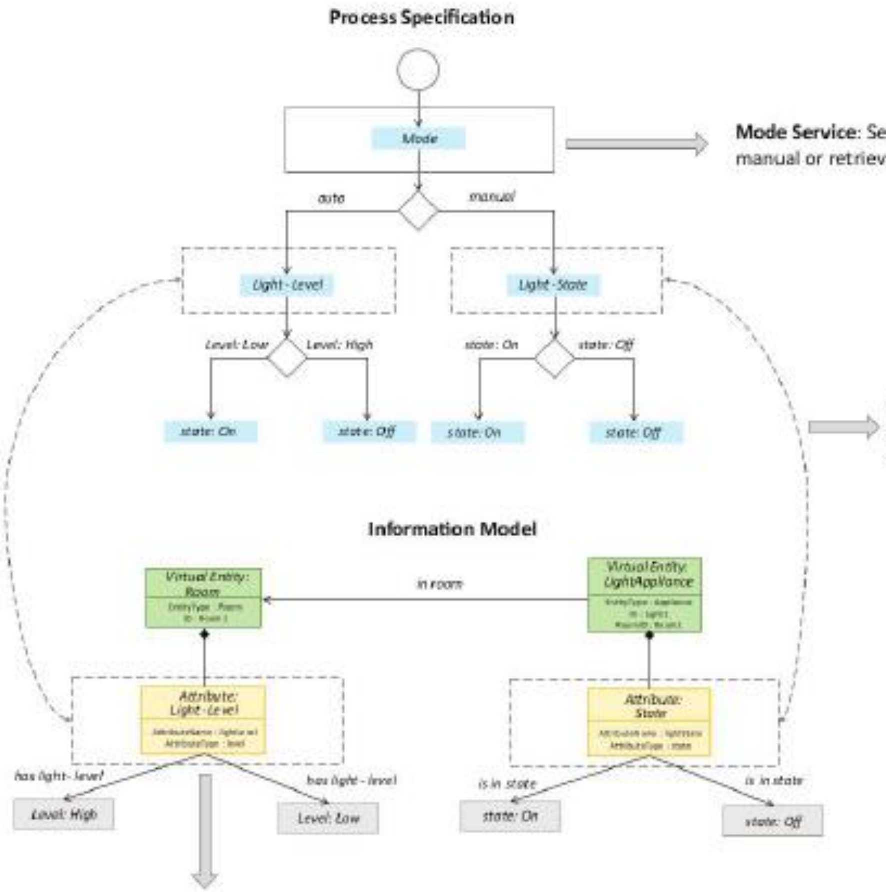
- The structure of all information in the IoT System like attributes, virtual entities, relations etc.,
- It adds more details to the virtual entities through their attributes and operations.

Information Model for Home automation IoT System



Service Specification

- Specifications about services like service schedules, service preconditions and service effects.
- From process specifications and information model states and attributes are identified.
- For Each state and attribute a service will be defined.

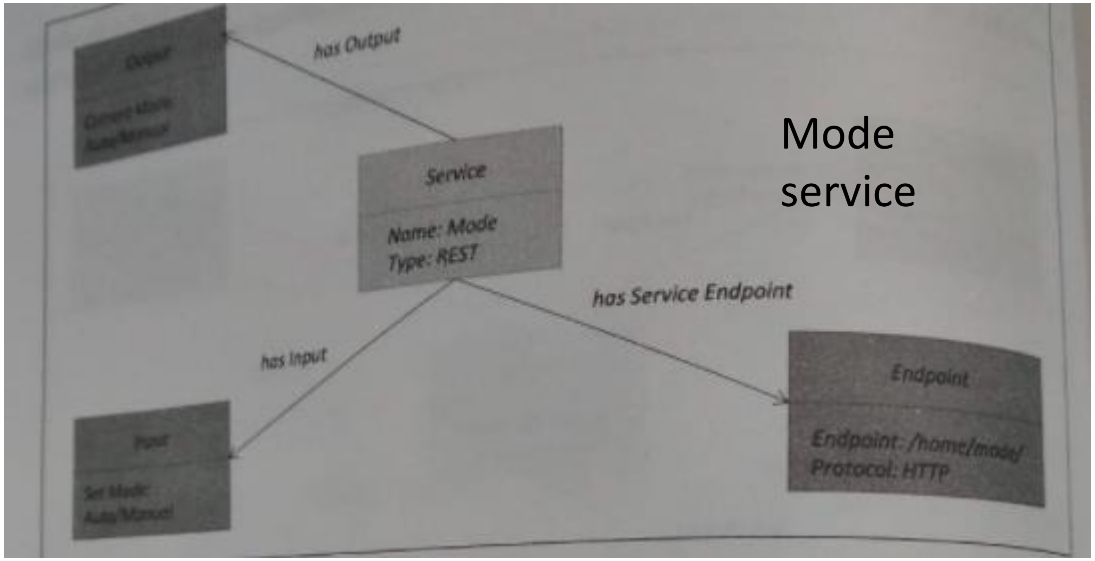


Mode Service: Sets mode to auto or manual or retrieves the current mode

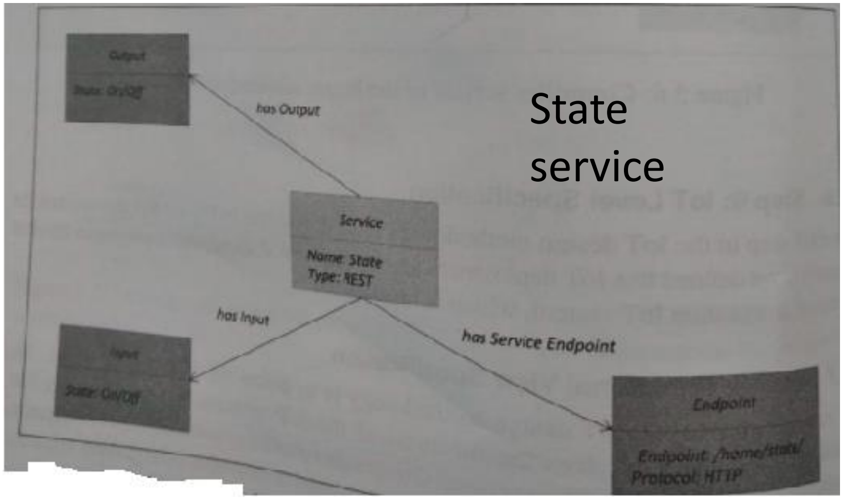
State Service: Sets the light appliance state to on/off or retrieves the current light state

Controller Service: In auto mode, the controller service monitors the light level and switches the light on/off and updates the status in the status database.
In manual mode, the controller service, retrieves the current state from the database and switches the light on/off.

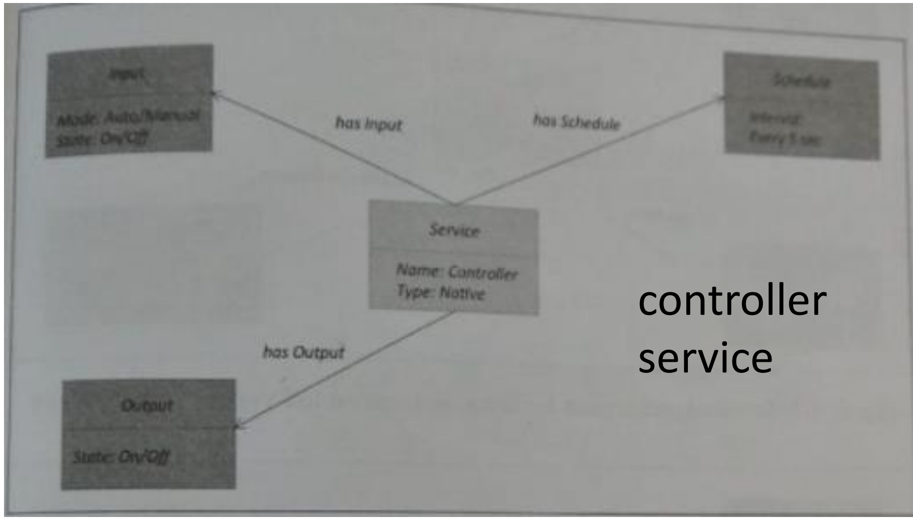
Service Specification for Home automation IoT System



Mode service

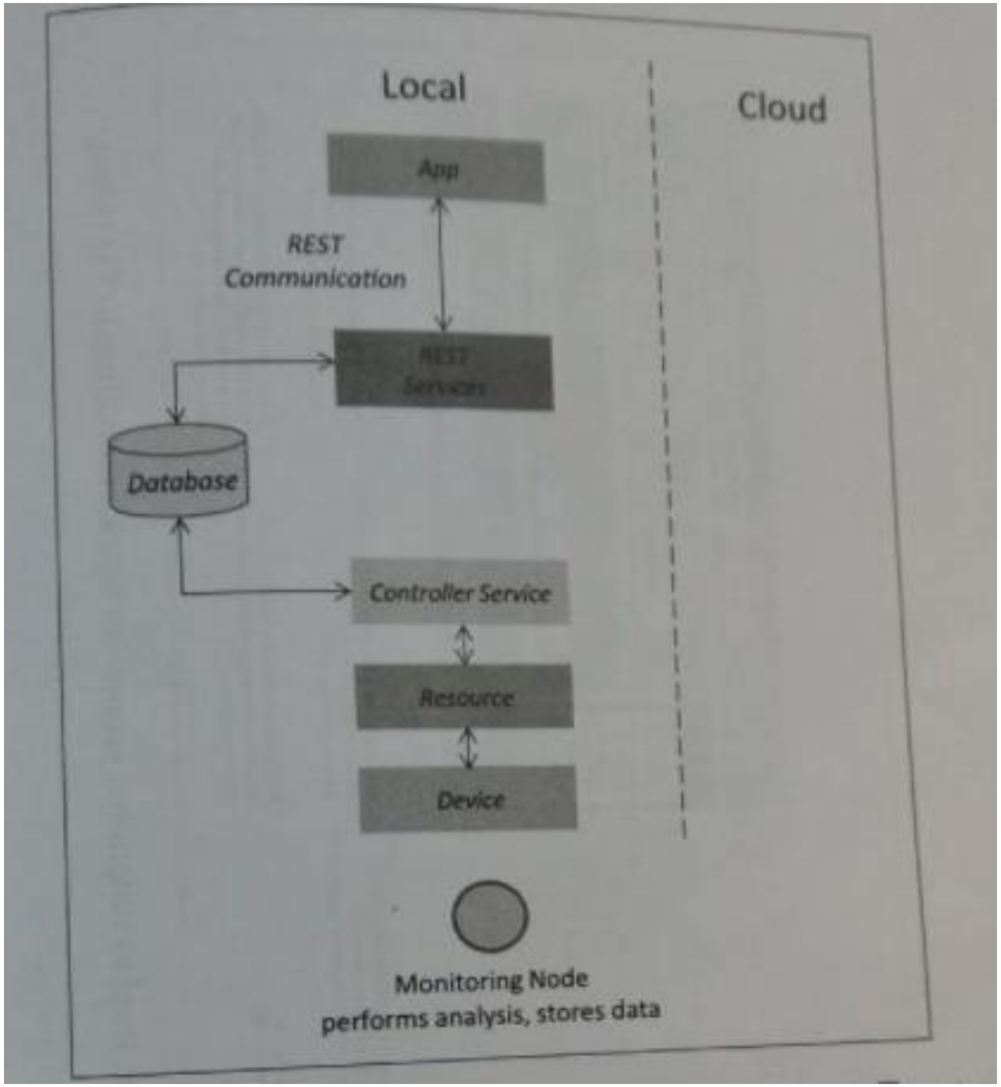


State service



controller service

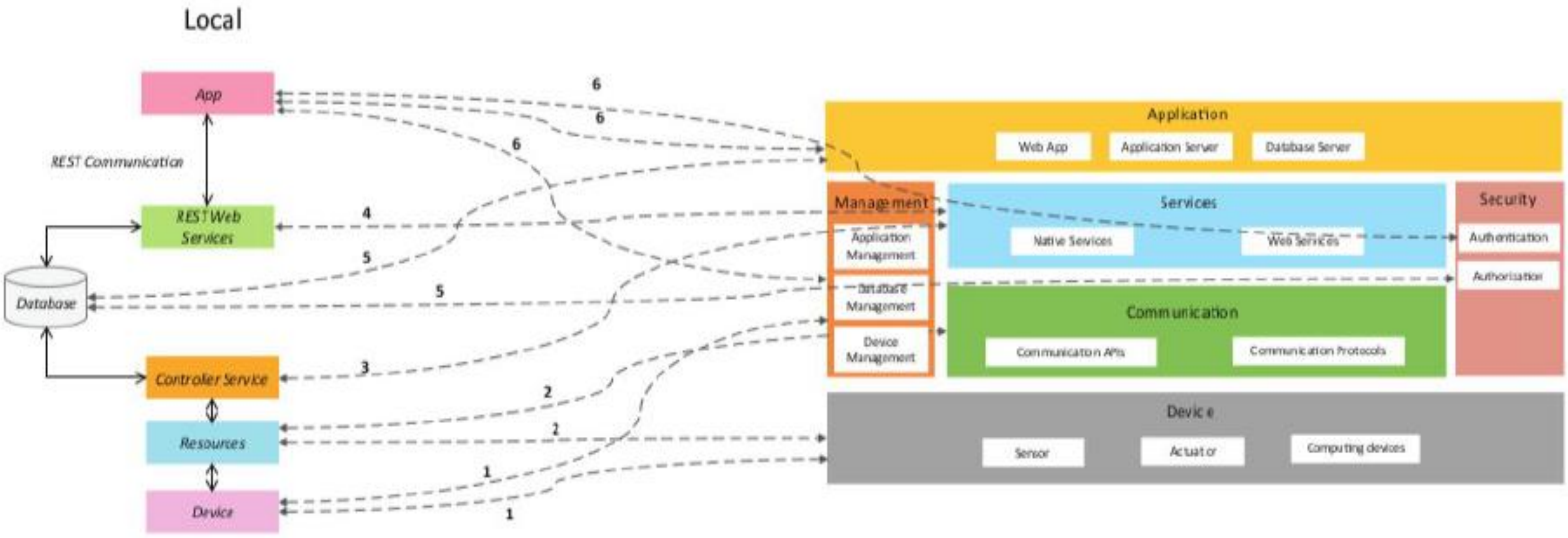
IoT Level specification



Function level specification

- About the functions of IoT system grouped into various functional groups(FG).
- Each FG provides functionalities to interact with the instances of concepts defined in Domain model or provides information related to the concepts.
- FG are
  - Device
    - Contains devices for monitoring and control.
    - For home automation system single board mini-computer, light and a relay switch.
  - Communication
    - Communication of IoT system like communication protocols that enables network connectivity.
    - Communication APIs
  - Services
    - Various services for device monitoring, device control service, data publishing and service discovery services.
    - REST and native services used for home automation system.
  - Management
    - Functionalities required for authentication and manage the IOT system.
  - Security
    - Security like authentication, data security and authorization.
  - Application

Function level specification for home automation system



1. IoT device maps to the Device FG (sensors, actuators devices, computing devices) and the Management FG (device management)

2. Resources map to the Device FG (on-device resource) and Communication FG (communication APIs and protocols)

3. Controller service maps to the Services FG (native service). Web Services map to Services FG (web services)

4. Web Services map to Services FG (web services)

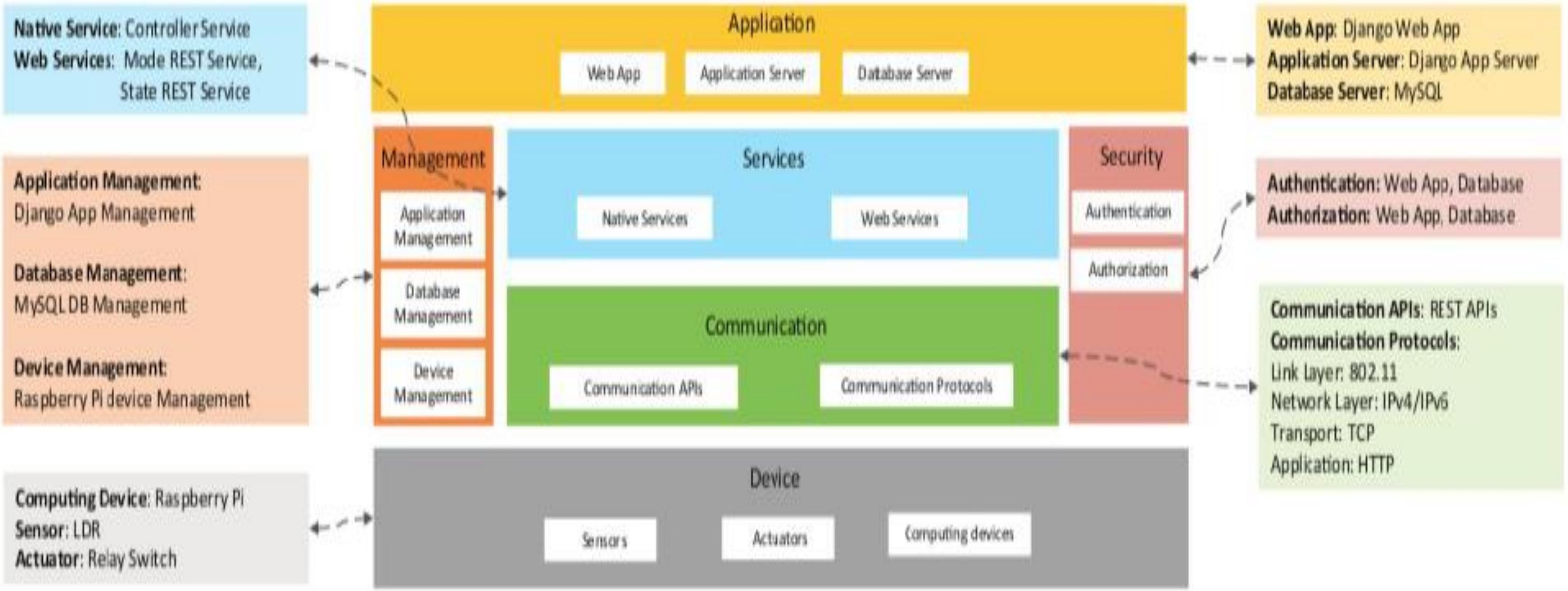
5. Database maps to the Management FG (database management) and Security FG (database security)

6. Application maps to the Application FG (web application, application and database servers), Management FG (app management) and Security FG (app security)

Operational view specification

- Options for pertaining to IoT system deployment and operation
  - Service hosting options, storage options, device options, application hosting options etc.,
- Devices: computing device (Rasberry Pi),light dependent sensor. Communication APIs, REST API & Communication Protocols: Link Layer-802.11, Network Layer-IPV4/IPv6,
- Services
  - Control services : Hosted on devices implemented in Python and run as a native service.
  - Mode services
  - State service:
- Applications
- Security
- Management

Operational view specification for home automation IoT system



Native Service: Controller Service
Web Services: Mode REST Service, State REST Service

Application Management: Django App Management

Database Management: MySQL DB Management

Device Management: Raspberry Pi device Management

Computing Device: Raspberry Pi
Sensor: LDR
Actuator: Relay Switch

Application

Web App

Application Server

Database Server

Management

Application Management

Database Management

Device Management

Services

Native Services

Web Services

Communication

Communication APIs

Communication Protocols

Security

Authentication

Authorization

Device

Sensors

Actuators

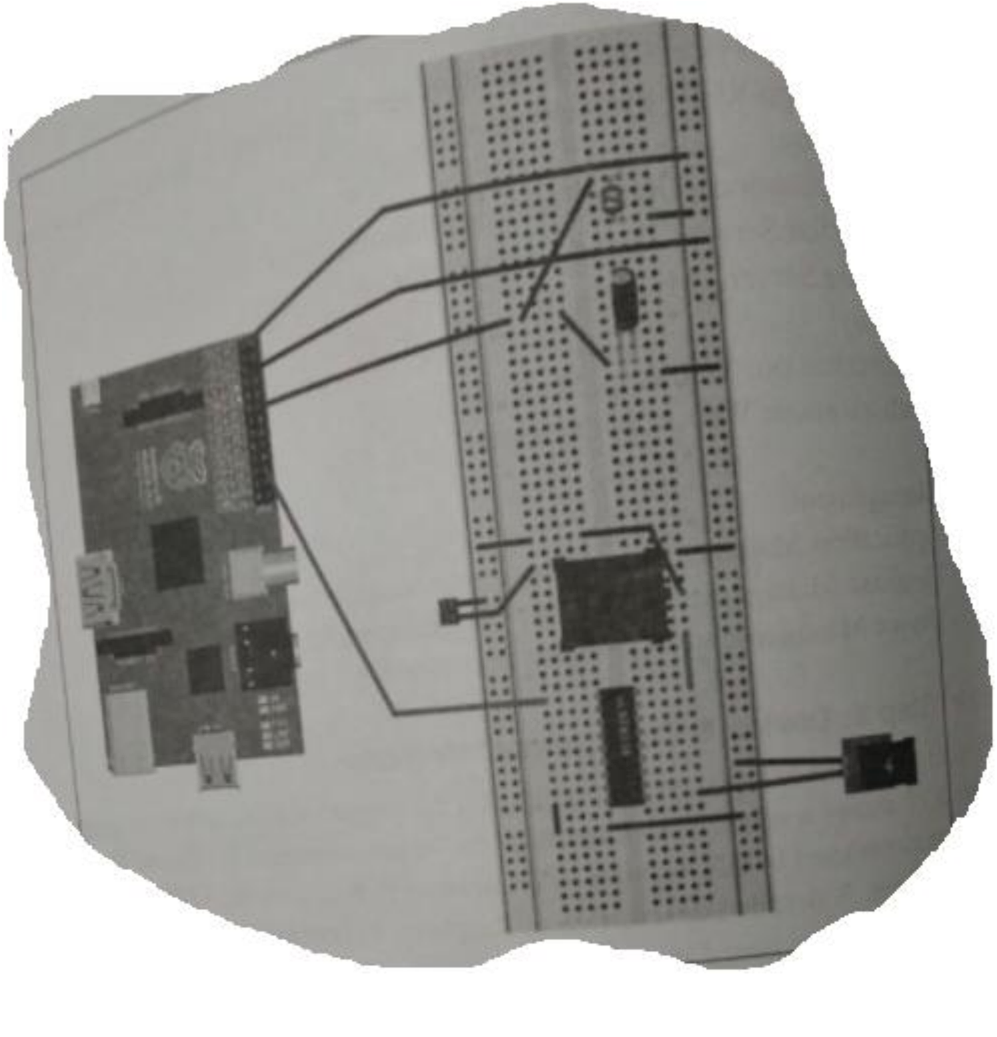
Computing devices

Web App: Django Web App
Application Server: Django App Server
Database Server: MySQL

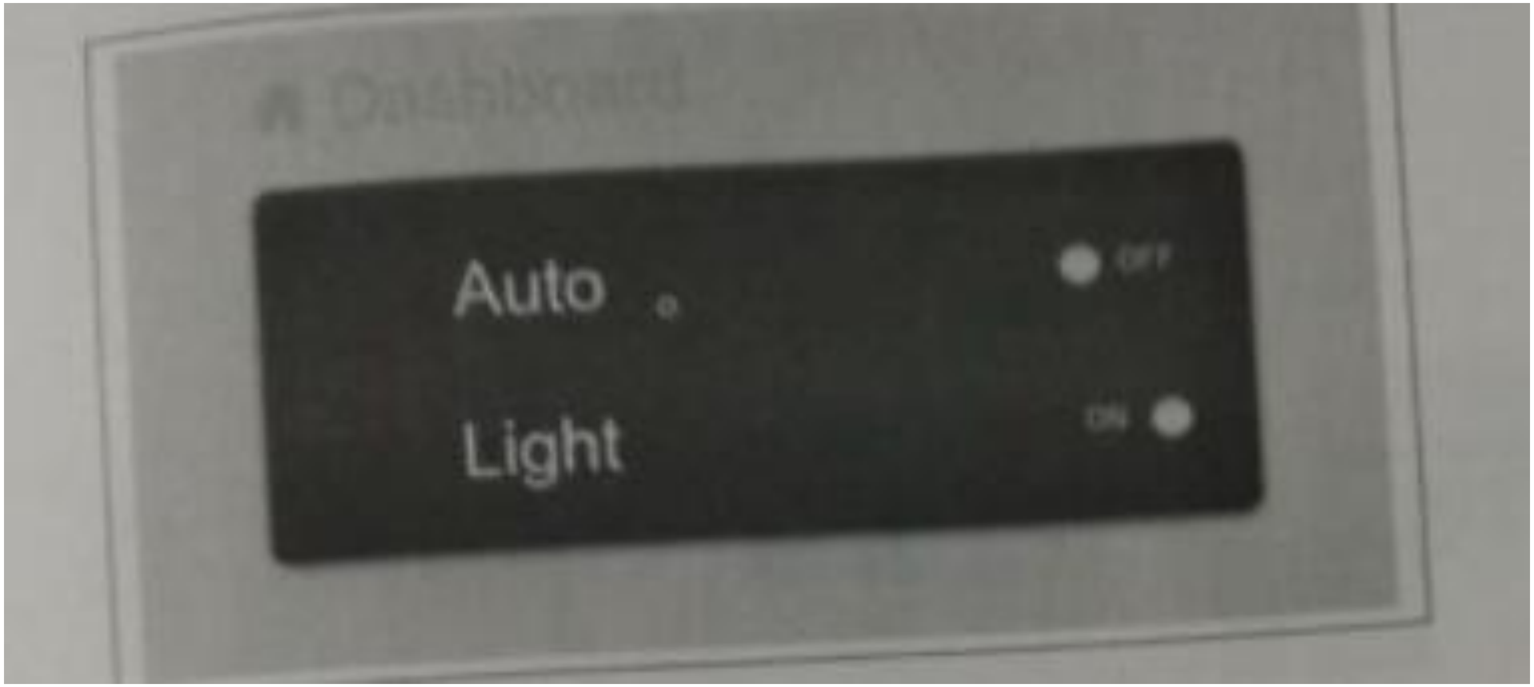
Authentication: Web App, Database
Authorization: Web App, Database

Communication APIs: REST APIs
Communication Protocols:
Link Layer: 802.11
Network Layer: IPv4/IPv6
Transport: TCP
Application: HTTP

Device & component integration



Application Development



Dashboard

Auto ● OFF

Light ON ●

Need and Goals for IoT solution

10 key factors for successful IoT solutions

1. Keep it simple

- Maintain simplicity in design and functionality to improve user acceptance and adoption.
- Additionally, reduce complexity in components to a minimum to make repairs and maintenance easier.

2. Demonstrate/prove the Business Value

- Develop clear objectives and use cases to effectively demonstrate the tangible business value of the solution.
- A successful IoT solution should be in sync with business goals and strategic priorities.
- The use cases should effectively demonstrate how the IoT solution positively impacts internal and external work processes, addresses challenges, and opens opportunities to generate competitive advantages in the market.

3. Start with scalability in mind from day 1

- Establishing **scalability as a foundational principle facilitates organic expansion**,
- not only to respond to the market's evolving demands
- but also to decide which partners, infrastructure, and connectivity layers are adequate for the solution.

4. Data security and hosting location

- Make sure to **use best-in-class software with proven security credentials**,
- as well as suppliers who can provide good security documentation and certification.
- Additionally, ensure that all legal documentation is adjusted to the legal system of the country in question.

5. Incorporate Best-in-Class components

- When it comes to IoT, it's important to **prioritize excellence over novelty** to ensure optimal performance.
- Given the ever-evolving nature of IoT, it's crucial to use top-tier components and partner with reliable companies with a proven track record and strong support.

6. Remote management of physical assets

- Cultivate proficiency in remotely monitoring, managing and optimizing the solution's hardware and software.
- To achieve this, invest in alerts and components that enable easy remote access to IoT infrastructure,
- allowing for **prompt decision-making or configuration based on up-to-date insights.**
- This factor is necessary to achieve scalability with a simplified approach.

7. Ease of deployment in end-user environments

- Prioritize a **simplified client onboarding process.**
- This way, the solution streamlines the assimilation process, minimizes costs, and reduces installation friction.
- This factor should also be applied to internal use-cases to secure smoother integration into workflows and enhanced productivity.

8. Adding layers of value

- Diversify the value of the solution by adding enhancements that increase its utility and responsiveness to the evolving needs of clients,
- whether they are external customers or internal departments within the organization.
- **Go beyond the technical aspects of the solution to open up more market opportunities** by making the proposal more comprehensive, innovative, and therefore, more attractive to potential clients.

9. Enhanced end-user experience

- When designing an IoT solution, it should be **easy to use, intuitive, and accessible to users** of all knowledge levels.
- It is important to consider the feedback of end-users in order to continually improve and remain relevant in meeting their expectations.

10. Collaborative work

- Developing a successful IoT solution requires **specialized skills, knowledge, and experience that should come from both internal and external suppliers.**
- Cultivating a strong collaborative philosophy around the solution allows for early access to new market opportunities,
- risk mitigation with limited resources, and the ability to pivot quickly to changing project requirements or market demands.

https://www.loriot.io/blog/10-factors-for-successful-iot.html

Adoption to IoT Solutions

Why IoT Adoption?

- IoT devices create multiple interaction points along supply chains that provide advanced data collection, factory automation, GPS shipment tracking, and enhanced communication between machines and people.
- The platform leverages years of experience and analytics to automate and enhance IoT, using unique solutions to enable connections to digital systems and devices
- It aims to help businesses make better decisions through the use of data.
- companies and enterprises can improve their IoT automation process
- streamline a lot of different areas in IoT adoption:
  - Allowing fast and accurate analyses
  - Improving security
  - Managing and obtaining insights from the data
  - Allowing better customizations, especially when it comes to data privacy
- Edge computing significantly improves the way companies and enterprises collect and analyze their data, as it processes information near the source, not in the cloud.
  - edge computing allows companies to make data-driven decisions

Reasons for IoT Adoption technologies

- **Eliminates dependency on complicated infrastructure**
- **Provides equal access to data**
- **IoT Depends on Advanced Cloud Technology**
- **Ongoing Disruptions Will Drive IoT Adoption**
  - **Pandemic**

Evaluation of IoT costs

These costs will vary depending on the scale of implementation, the complexity of the devices, and the specific use cases.

Costs components

- Initial Hardware and Setup: Installation of sensors, gateways, and network connectivity.
- Software and Platforms: IoT management platforms, cloud storage, and analytics tools.
- Maintenance: Regular updates and physical maintenance of devices.
- Security: Cybersecurity solutions and compliance with regulations.
- Scalability and Operations: Training, change management, and potential expansion costs.

Initial Hardware and Setup

- Hardware Costs:
  - Sensors and Devices: These are the actual IoT devices, such as sensors, actuators, smart meters, or cameras, which collect and transmit data.
  - Connectivity Modules: Devices need modules to communicate, including Wi-Fi, Bluetooth, Zigbee, or cellular modules.
- Edge Devices & Gateways: Hardware that aggregates data from sensors before transmitting to the cloud or data centers.
- Computing Infrastructure: This may include local servers, gateways, or edge computing solutions to manage and process IoT data.
- Installation and Deployment:
  - Physical Setup: This includes the cost of physically installing sensors, wiring, and configuring devices to work together.
  - System Integration: Customization to ensure that the IoT system integrates with existing IT infrastructure, which might require consultation or engineering expertise.

Software and Platform Costs

- IoT Platforms: These are software platforms for device management, data analytics, visualization, and monitoring. Platforms may charge a subscription fee or license fee.
- Custom Software Development: Depending on the use case, companies may need to develop custom applications to process and analyze data, or to create user interfaces.
- Security Solutions: Implementing strong encryption, secure communication channels, and access control will add additional software-related costs.

Connectivity Costs

- Network Costs: Depending on the number of devices and the type of data being transmitted, IoT solutions may require robust, continuous internet connectivity (Wi-Fi, cellular, satellite, etc.), which adds data subscription fees.
- Bandwidth Usage: More devices generating data lead to higher bandwidth consumption, especially for devices that transmit large volumes of data (e.g., video).

Maintenance and Management Costs

- Device Maintenance: IoT devices, especially those installed in remote or hard-to-reach areas, require regular maintenance, battery replacement, or hardware updates.
- System Updates and Patches: Regular software updates, security patches, and firmware upgrades are necessary to keep the system secure and functional.
- Data Management: Large-scale IoT adoption generates huge amounts of data that need to be stored, processed, and analyzed. Costs include data storage (cloud or on-premise), data processing, and analytics tools.

Security Costs

- Cybersecurity Solutions: IoT networks are vulnerable to cyber threats, so security investments like intrusion detection systems, firewalls, data encryption, and access management solutions are necessary.
- Compliance and Regulation: Some industries (like healthcare or finance) have strict data privacy and security regulations (e.g., GDPR, HIPAA), which could require compliance investments.

Training and Operational Costs

- Training Staff: Employees need to be trained to manage and maintain IoT systems, interpret data, and use new platforms.
- Change Management: Adoption of IoT technology often requires changes in workflows or business processes, leading to additional costs for organizational restructuring or business process reengineering.
- Support and Troubleshooting: Post-deployment, IoT systems need support services for troubleshooting, regular maintenance, or resolving connectivity and operational issues.

Data Analytics and Insights

- Advanced Analytics Tools: For larger deployments, IoT data might be fed into AI or machine learning platforms, which can be costly depending on the sophistication of the algorithms and processing power needed.
- Cloud Services: Most IoT systems rely heavily on cloud-based data storage and analytics. This often requires ongoing cloud service subscriptions (e.g., AWS, Azure IoT Hub, Google Cloud IoT).

Scalability Costs

- Expansion Costs: As IoT adoption grows, businesses might need to scale their systems, requiring investment in additional devices, connectivity, and computing power.
- Infrastructure Upgrades: Additional costs might arise if existing infrastructure (network, servers, etc.) needs to be upgraded to handle larger IoT deployments.

References

- https://innovationatwork.ieee.org/discussing-iot-adoption-benefits-and-distribution/
- https://1nce.com/en-eu/resources/news-insights/blog/iot-project-planning

Need and Goals for IoT solution

10 key factors for successful IoT solutions

1. Keep it simple

- Maintain simplicity in design and functionality to improve user acceptance and adoption.
- Additionally, reduce complexity in components to a minimum to make repairs and maintenance easier.

2. Demonstrate/prove the Business Value

- Develop clear objectives and use cases to effectively demonstrate the tangible business value of the solution.
- A successful IoT solution should be in sync with business goals and strategic priorities.
- The use cases should effectively demonstrate how the IoT solution positively impacts internal and external work processes, addresses challenges, and opens opportunities to generate competitive advantages in the market.

3. Start with scalability in mind from day 1

- Establishing **scalability as a foundational principle facilitates organic expansion**,
- not only to respond to the market's evolving demands
- but also to decide which partners, infrastructure, and connectivity layers are adequate for the solution.

4. Data security and hosting location

- Make sure to **use best-in-class software with proven security credentials**,
- as well as suppliers who can provide good security documentation and certification.
- Additionally, ensure that all legal documentation is adjusted to the legal system of the country in question.

5. Incorporate Best-in-Class components

- When it comes to IoT, it's important to **prioritize excellence over novelty** to ensure optimal performance.
- Given the ever-evolving nature of IoT, it's crucial to use top-tier components and partner with reliable companies with a proven track record and strong support.

6. Remote management of physical assets

- Cultivate proficiency in remotely monitoring, managing and optimizing the solution's hardware and software.
- To achieve this, invest in alerts and components that enable easy remote access to IoT infrastructure,
- allowing for **prompt decision-making or configuration based on up-to-date insights.**
- This factor is necessary to achieve scalability with a simplified approach.

7. Ease of deployment in end-user environments

- Prioritize a **simplified client onboarding process.**
- This way, the solution streamlines the assimilation process, minimizes costs, and reduces installation friction.
- This factor should also be applied to internal use-cases to secure smoother integration into workflows and enhanced productivity.

8. Adding layers of value

- Diversify the value of the solution by adding enhancements that increase its utility and responsiveness to the evolving needs of clients,
- whether they are external customers or internal departments within the organization.
- **Go beyond the technical aspects of the solution to open up more market opportunities** by making the proposal more comprehensive, innovative, and therefore, more attractive to potential clients.

9. Enhanced end-user experience

- When designing an IoT solution, it should be **easy to use, intuitive, and accessible to users** of all knowledge levels.
- It is important to consider the feedback of end-users in order to continually improve and remain relevant in meeting their expectations.

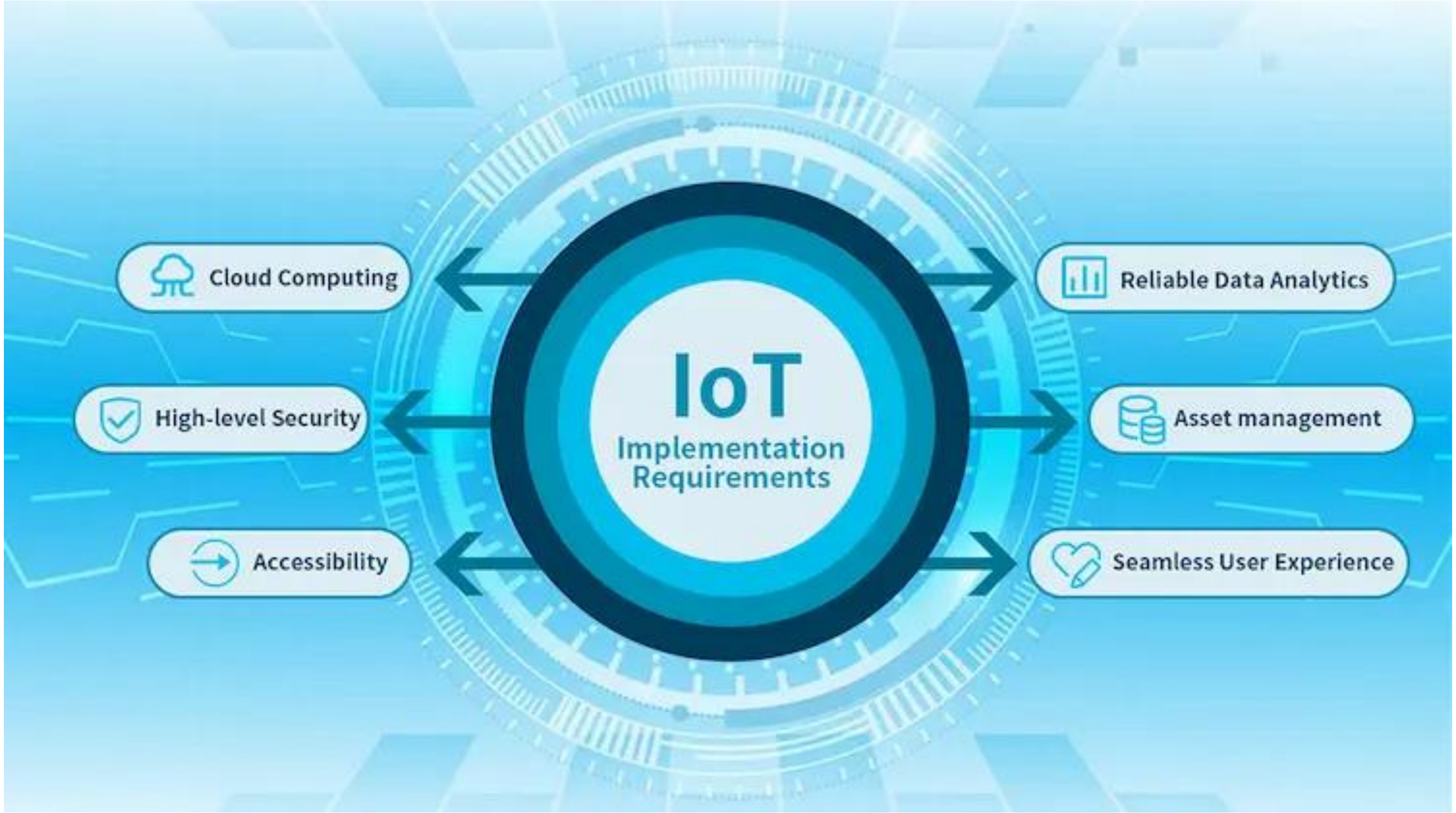
10. Collaborative work

- Developing a successful IoT solution requires **specialized skills, knowledge, and experience that should come from both internal and external suppliers.**
- Cultivating a strong collaborative philosophy around the solution allows for early access to new market opportunities,
- risk mitigation with limited resources, and the ability to pivot quickly to changing project requirements or market demands.

https://www.loriot.io/blog/10-factors-for-successful-iot.html

IoT Implementations Basics

IoT Solution Requirements

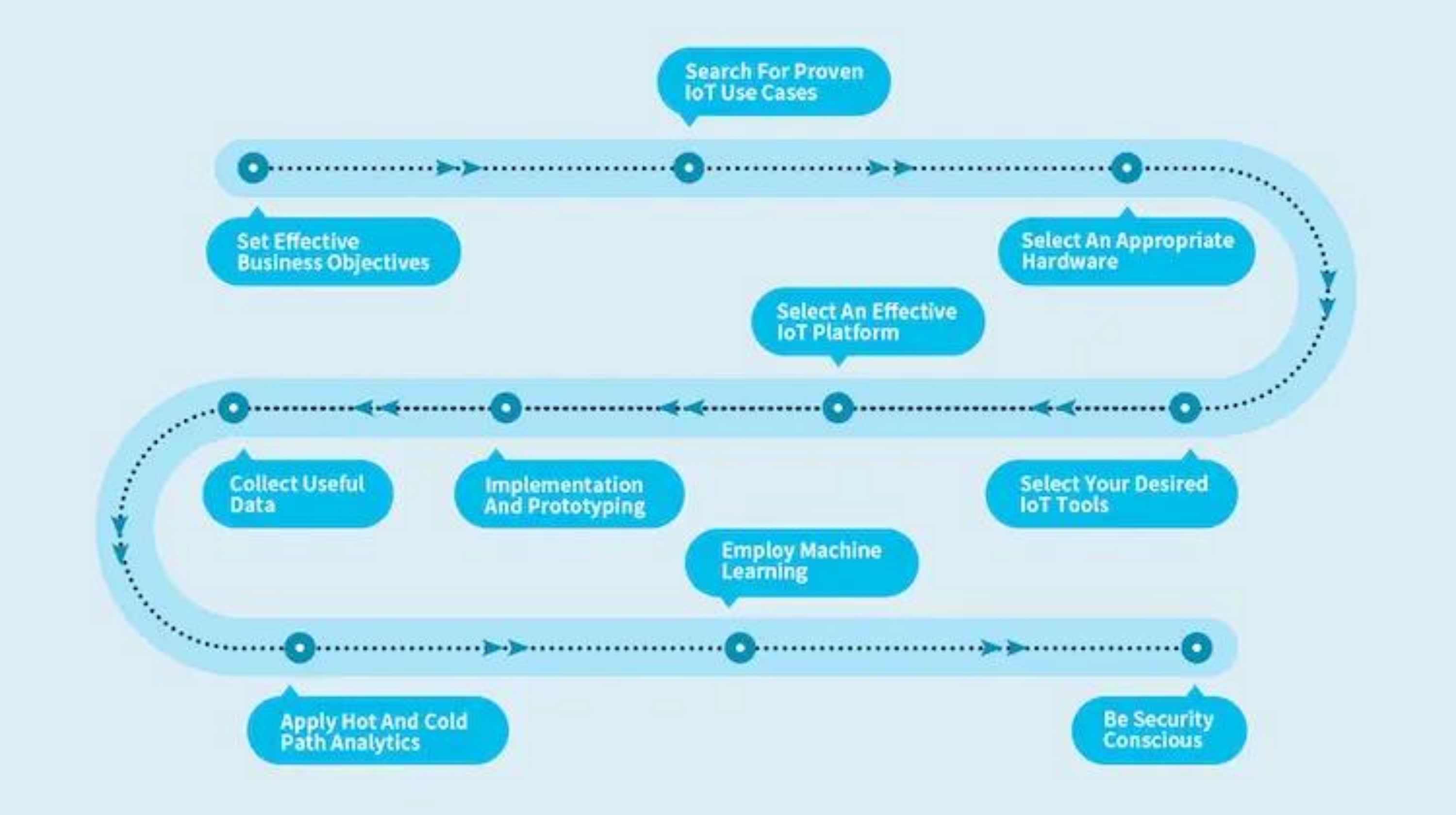


Plan for IoT Solutions
or steps for IoT Implementations

Steps

1. **Set Effective Business Objectives**
2. **Search For Proven IoT Use Cases**
3. **Select An Appropriate Hardware**
4. **Select Your Desired IoT Tools**
5. **Select An Effective IoT Platform**
6. **Implementation And Prototyping**
7. **Collect Useful Data**
8. **Apply Hot And Cold Path Analytics**
9. **Employ Machine Learning**
10. **Be Security Conscious**

Steps


Search For Proven IoT Use Cases
Set Effective Business Objectives
Select An Appropriate Hardware
Select An Effective IoT Platform
Collect Useful Data
Implementation And Prototyping
Select Your Desired IoT Tools
Employ Machine Learning
Apply Hot And Cold Path Analytics
Be Security Conscious

Set Effective Business Objectives

- it involves setting practical business objectives
- It defines the investments for a short or long period
- It clearly define your goals for IoT
- Must define:
  - The problem in the short and long term
  - The aim for solving the problem
  - The best way to solve the problem

Search For Proven IoT Use Cases

- It is an effective IoT implementation in research proven use cases.
- identify the loopholes in your business objectives and plans with IoT implementation.
- Some of the common tested use cases in this step includes:
  - Preventive Maintenance
  - Automatic Refilling
  - **Resource Micromanagement**
  - Asset Tracking And Management
  - Environmental Monitoring
  - **Design for IoT**
  - Access Control And Security
  - Process Control And Optimization

Select An Appropriate Hardware

- select appropriate hardware consisting of the most primary sensors for data collection include volume, weight, color, sound, vision, temperature, pressure, and humidity.
- A connection device to upload the data on the cloud.
- other devices, such as actuators and edge computers.
- Protocols for implementing IoT : 6LoWPAN, Zigbee, and Z-wave

Select Your Desired IoT Tools

- connect an IoT device to the internet for Collecting, processing, and sending sensor data to designated endpoints
  • Receive commands to set or do tasks and control actuators.
- Need to identify the various tools to predict user’s habits or wishes and notify them for the problems etc.

Select An Effective IoT Platform

- IoT platforms are software for centralizing and controlling all aspects of IoT devices and networks.
- these IoT platforms from specialized suppliers or custom-made in-house

Implementation And Prototyping

- It allows the thorough analysis for entire process.
- Before implementation identifying several tech professionals and assemble the team for testing the prototype.
- Some of the experts to include in the team consists of IT experts, telecommunications specialists, manufacturing experts, computer, software, electronic, mechanical, mechatronics, and automation engineers
- The team selected based on target for IoT.
- You need to write about various teams required for this stage.

Collect Useful Data

- generating terabytes of data daily.
- collecting sufficient and valuable data.
- Several sensors can be used for this; however, more complex needs would require more sensors for data collection.
- must be interpreted, processed, and stored on a secure database.
  - What are data points required for the IoT Solution

Apply Hot And Cold Path Analytics

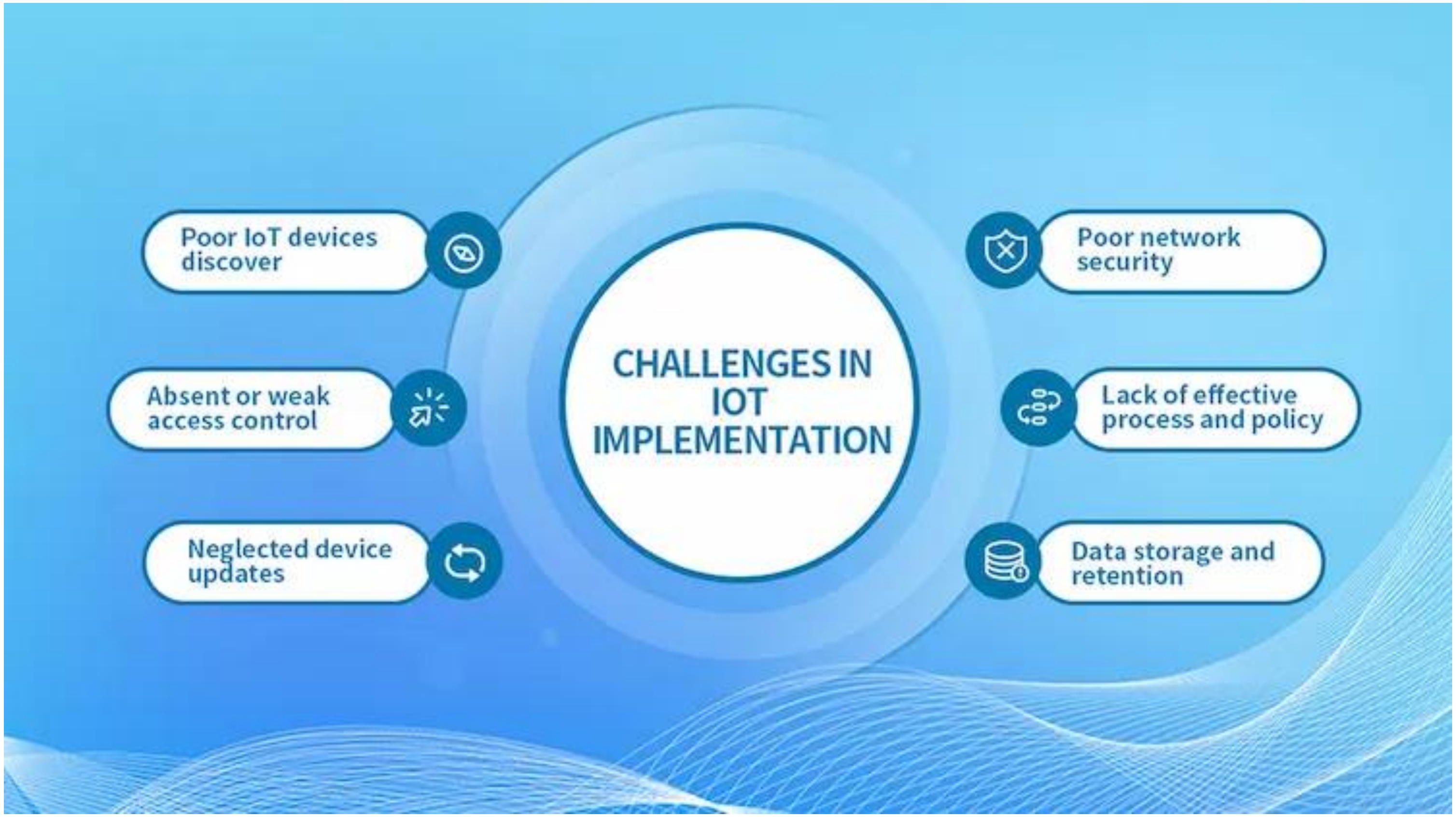
- It is for decision-making processes for better efficiency.
- Hot path analytics are short-term, while cold path analytics focuses on the long-term.
- The data is converted or interpreted by embedded systems and later analyzed.
- Hot and cold path analytics are analyses performed by data scientists, aided by machine learning software

Employ Machine Learning

- Machine learning involves using artificial intelligence to review information in real-time. It helps to identify patterns in the data and act on them.

Be Security Conscious

- Plan to protect your business from unforeseen attacks.
- deploy effective security measures that can protect your business from hacking and other attacks.



CHALLENGES IN IOT IMPLEMENTATION

Poor IoT devices discover

Absent or weak access control

Neglected device updates

Poor network security

Lack of effective process and policy

Data storage and retention

Poor IoT Device Discover

- the lack of adequate discovery of IoT devices.
  - Data can't be managed, becoming attack vectors for fraudsters and hackers to access the network efficientl
- ensure that all IoT tools and practices can configure all IoT devices within the environment.

Absent Or Weak Access Control

- It is about weak access control of devices and products.
- Weak authentication and authorization leads to unprivileged access of devices and networks
- Ensure the robustness of network’s security measures.
- Including unique ID to each device to enhance the access control.
- Configure each device with least privilege to have the best access control.

Neglected Device Updates

- IoT devices could be susceptible to hacking and intrusion if the updates are overlooked or neglected.
- Periodically, IoT devices patches or updates to internal firmware and other software is required.

Poor Network Security

- deployments regularly add thousands of devices, which are all connected to a LAN and to IoT VPN networks.
- With every device connected to the LAN, a potential access point for hacking or intrusion is opened.
- additional network-wide security protocol must be deployed to implement IoT effectively like intrusion preventions and detection systems, powerful antimalware tools.

Lack Of Effective Process And Policy

- It deals about the effective practices and tools used for configuring, enforcing, and monitoring IoT device security throughout the network.
- Everyday IoT security processes and policies must be recognized to solve the lack of effective policies.
- Clear configuration guidelines, proper documentation, rapid response, and reporting are examples of IoT security processes.

Data Storage And Retention

- The data produced by IoT devices is a valuable asset.
- The data stored is highly time-sensitive.
- lack the capacity or struggle to keep such enormous data effectively.
- better tools must be provided to appropriately store and secure these data

References

- https://www.mokosmart.com/iot-implementation-guide/