# Internet of Things

## An Overview of Enabling Technologies, Protocols and Use Cases

Reza Vahidnia

Fall 2023

# Topics

1. Introduction to IoT
2. Solution Architecture
3. Smart Devices
4. Application Protocols
5. Access Technologies
6. Platforms
7. Security
8. Data Handling
9. Artificial Intelligence of Things
10. Applicability

Lecture 1

# Introduction to IoT

# Genesis of IoT


**Connectivity**

Digitize Access
- Email
- Web Browser
- Search

**Network Economy**

Digitize Business
- E-commerce
- Digital Supply Chain
- Collaboration

**Immersive Experiences**

Digitize Interactions
- Social
- Mobility
- Cloud
- Video

**Internet of Things**

Digitize the World
- People
- Process
- Data
- Things

## Evolutionary phases of the Internet

IoT is poised to change our world in new and exciting ways, just as the past Internet phases already have.

# What Made IoT Possible?

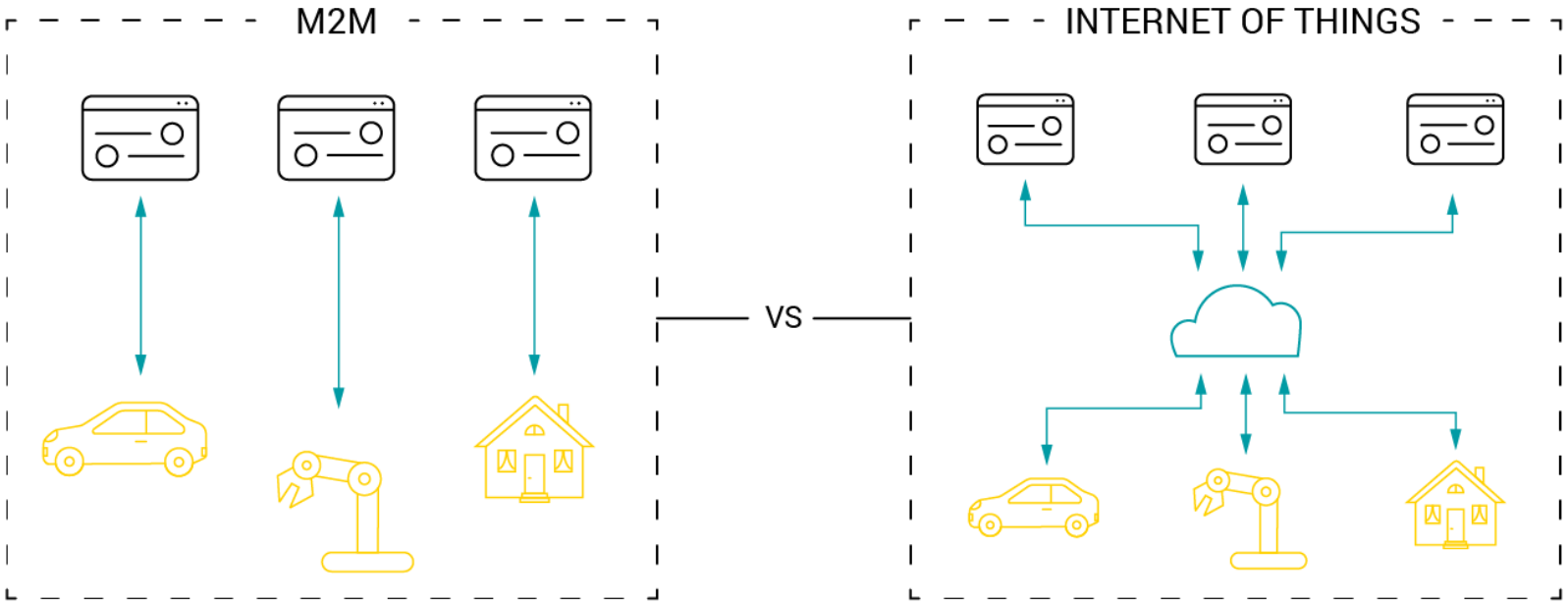

**Low-cost, Low-power Sensors**

**Connectivity & Protocols**

**Cloud Computing Platforms**

**Artificial Intelligence, Machine Learning & Analytics**

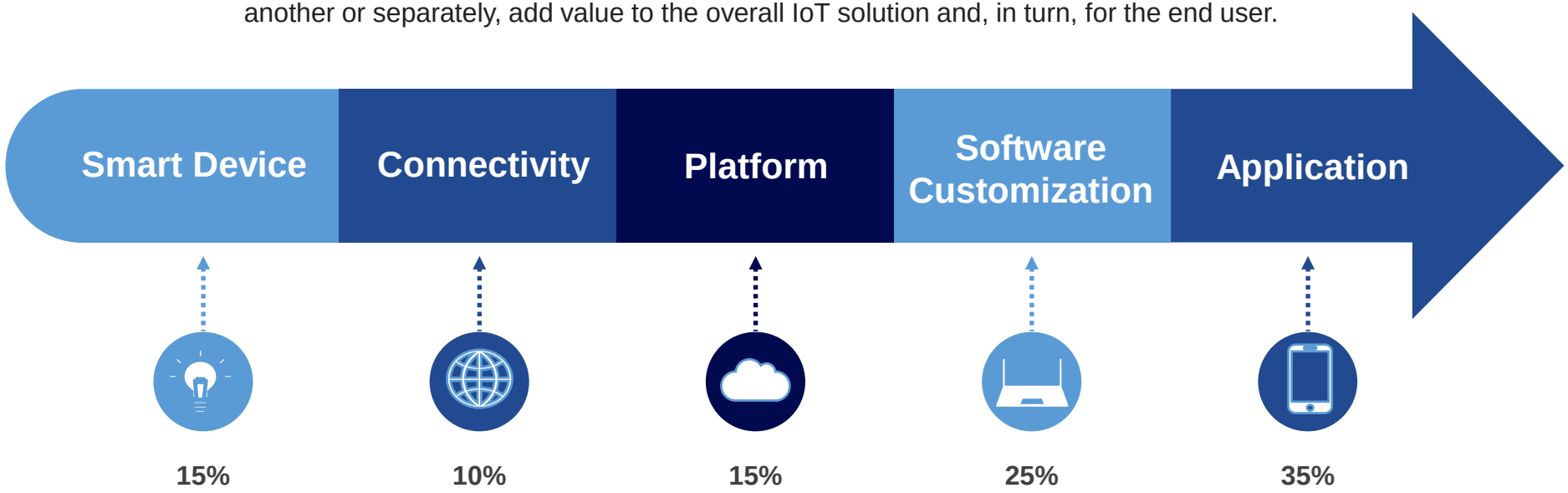
# IoT vs. M2M




| M2M | IoT |
| --- | --- |
| Simple device-to-device communication usually within an embedded software at client site | Grand-scale projects and want-it-all approach |
| Isolated systems of devices using same standards | Integrates devices, data and applications across varying standards |
| Limited scalability options | Inherently more scalable |
| Wired or cellular network used for connectivity | Usually devices require active Internet connection |
| Extensive background of historical applications | State-of-the-art approach with roots in M2M |

# IoT Value Chain

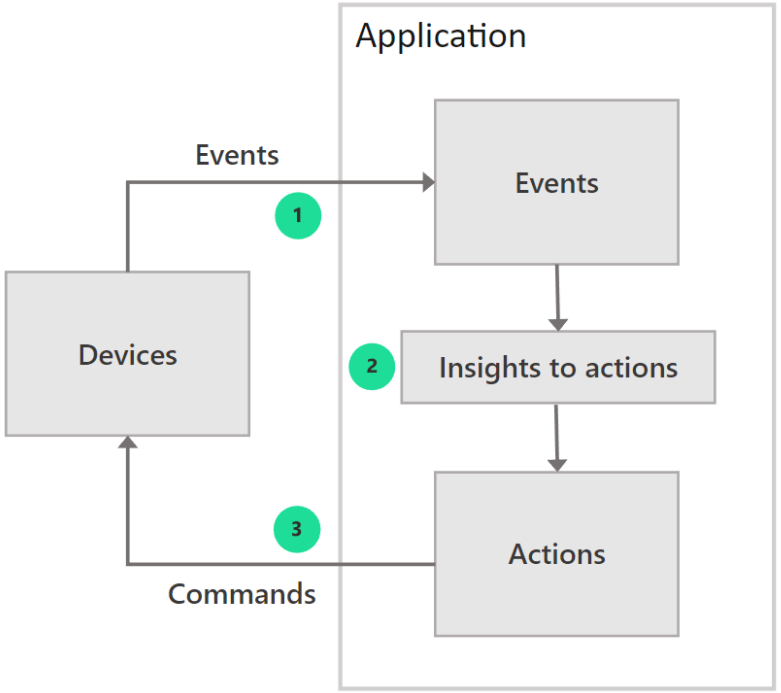
The IoT value chain illustrates how the different components, in combination with one another or separately, add value to the overall IoT solution and, in turn, for the end user.

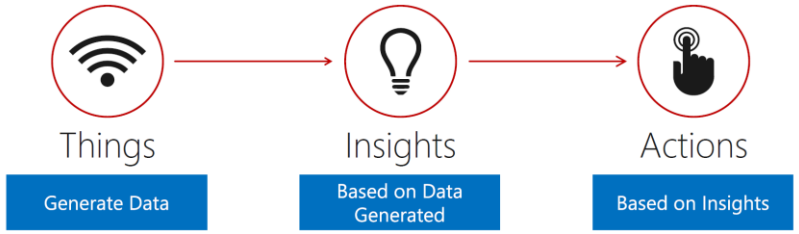


# IoT Conceptual Overview

The basic goal of IoT is to **connect the "Things"** to derive **actionable insight**.

1. **Events:** Devices generate events and send them to cloud applications.
2. **Insights:** Applications derive insights by evaluating data from incoming device events.
3. **Actions:** Based on insights, applications take action by running processes and workflows. Applications can also send commands to the devices.



# IoT Conceptual Overview

**1: Events:** represent device-to-cloud communication in an IoT solution, and can be notifications, acknowledgments, or telemetry.

**Notifications**

- Alerts from devices that are malfunctioning.
- Device state or property change updates.
- Requests to provide information.

**Acknowledgments**

- Progress updates on long-running requests.
- Success or failure signals for completing an asynchronous request.

**Telemetry**

- Continual sensor data from devices to applications.
- Monitored health and diagnostics data from devices.
- Regular location data from tracked assets.

# IoT Conceptual Overview

**2: Insights:** are interpretations of events.

### Contextual

**Context-sensitive interpretations of events**

- Where to route a message, based on contextual data like message header content or device type.
- Runtime decisions by event handling code that decides whether to take immediate action based on an event.
- Reconciling acknowledgments to complete stateful transactions.

### Real-time

**Gathered and observed in real-time for monitoring and decision-making.**

- Gathering and observing near real-time solution metrics.
- Monitoring solution health for visualization, alerting, and remediation.
- Combining events with other data sources for real-time transformation and output to display and analyze.

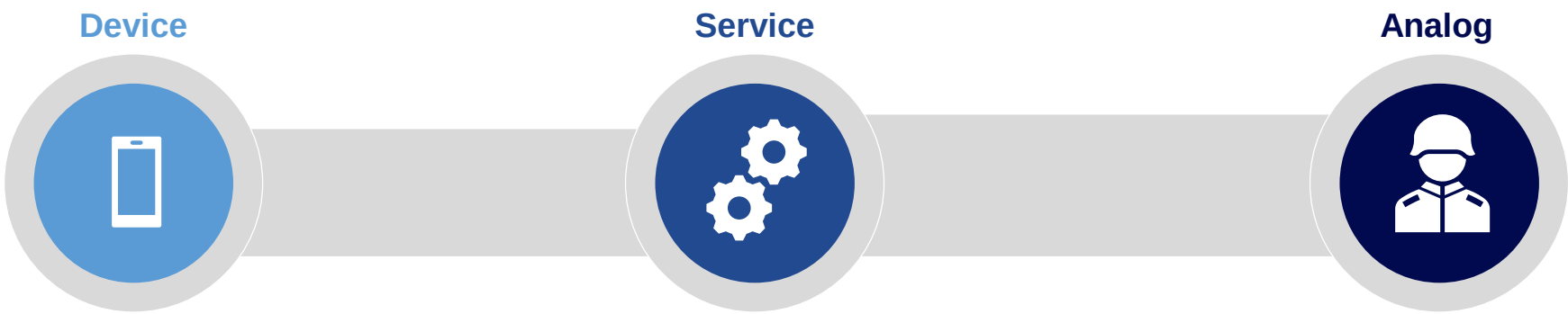
### Aggregated

**Batch processing on aggregated data.**

- Building training data for ML and AI to improve device and service algorithms.
- Gathering and observing trends and characteristics over long durations to use for improving processes.

# IoT Conceptual Overview

**3: Actions:** are deliberate activity undertaken either programmatically or manually as *device*, *service*, or *analog* actions.




**Instructions or information an IoT application sends to a device to act on locally.**

- Commands sent to control a device.
- Configuration data sent to a device to modify its behavior.
- On-demand requests to a device to provide data or state.

**Service or intro-process communications that one part of a solution sends to another.**

- Requests for data from external services to use in solutions.
- Transactions with other services as part of application logic.
- Summoning emergency, police, or other external services.

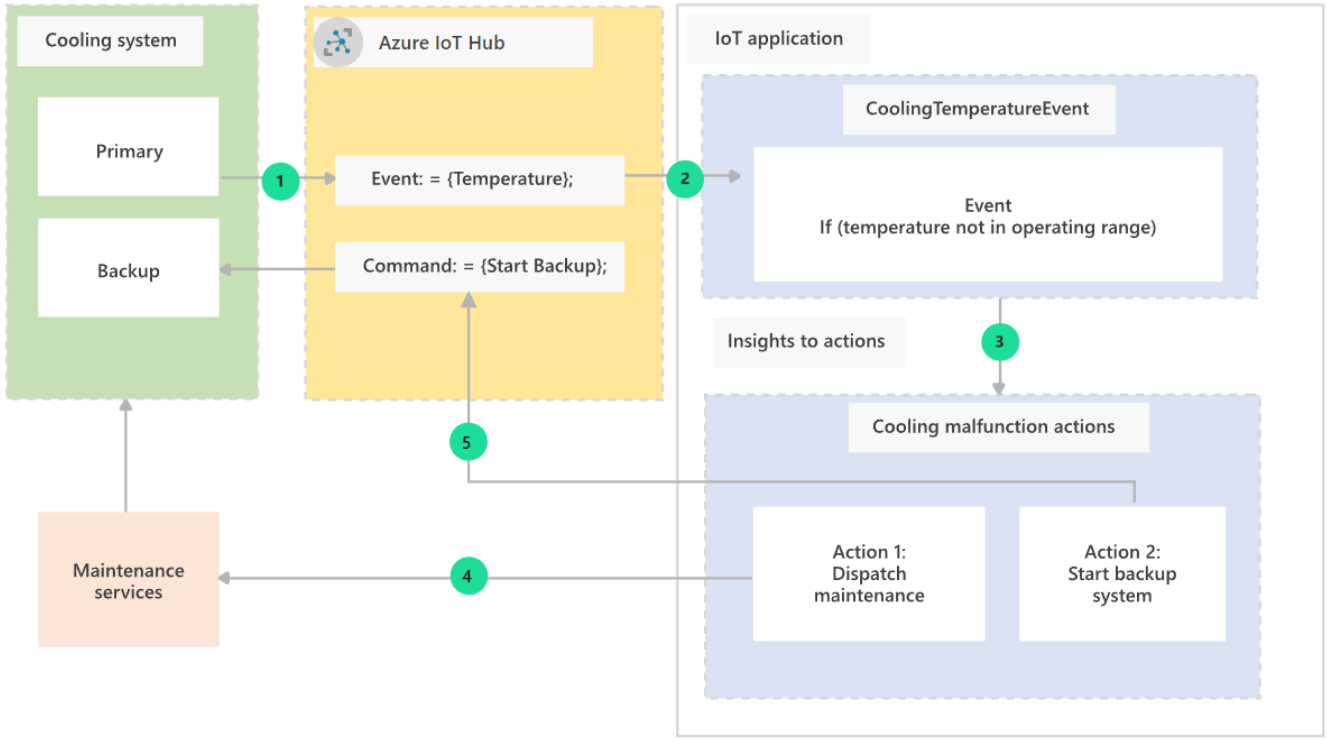
**Tracking analog actions happening outside of solution automation as part of a workflow**

- Field operators notifying a solution when they complete a requested task.
- Human-conducted scoring and tuning of training data for AI.

# IoT Conceptual Overview

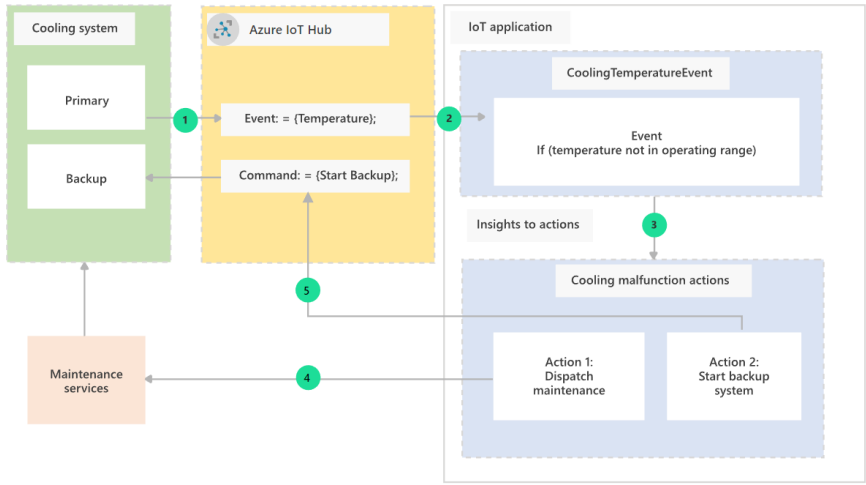
**Example:** Interaction of events, insights, and actions in a food storage temperature monitoring IoT solution.

1. Device sensors send operating temperatures as telemetry to a connected application through IoT Platform.
2. The cloud application monitors temperatures, and takes actions if the temperature gets too low or high.
3. Devices can receive commands to adjust temperatures or start and stop operation.
4. There are backup systems in case a primary system malfunctions or goes offline.



# IoT Conceptual Overview

**Example:** Interaction of events, insights, and actions in a food storage temperature monitoring IoT solution.

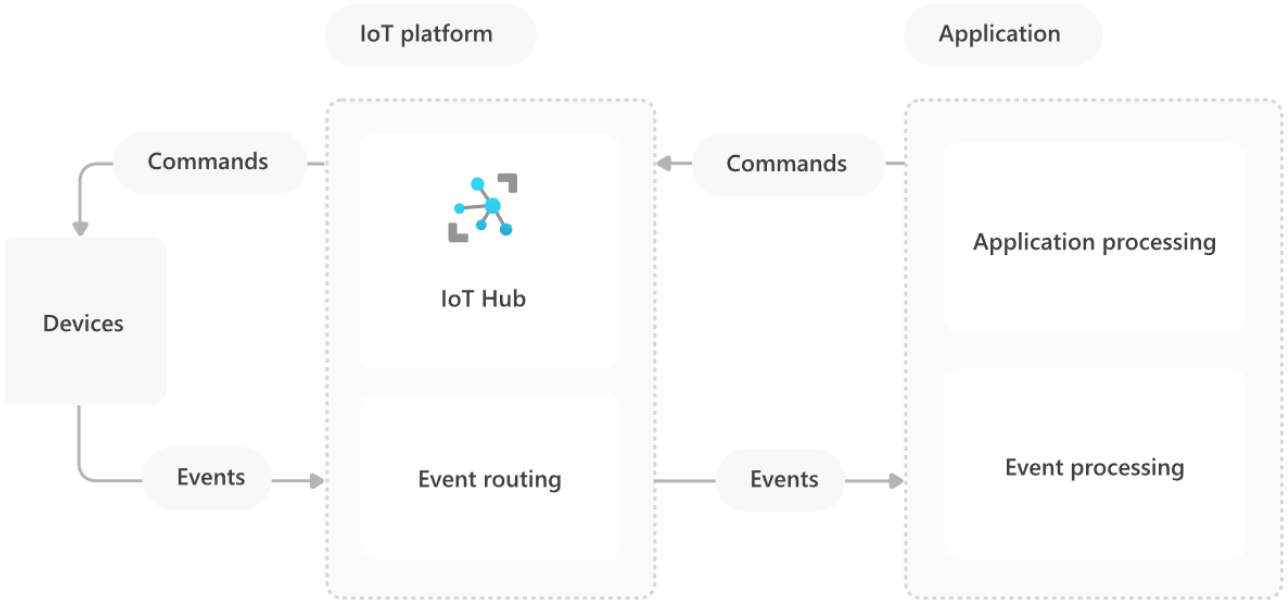



| Event | Insight | | Action | |
|---|---|---|---|---|
| Report single event with temperature out of operating range. | **Contextual** | Single event.<br>Cooling system malfunction. | **Service** | Invoke maintenance service dispatch. |
| Monitor and analyze real-time events for operating temperature anomalies. | **Real-time** | Several events.<br>Temperature needs adjustment to stay in range. | **Device** | Notify devices to adjust temperatures. |
| Gather events over many days to analyze ongoing maintenance patterns. | **Aggregated** | Many events.<br>Malfunctions happen more often during certain periods. | **Analog** | Modify regular system maintenance schedule. |

# IoT Structural Components

IoT solutions are a collection of assets and components divided across:

- IoT devices
- IoT platform
- IoT applications



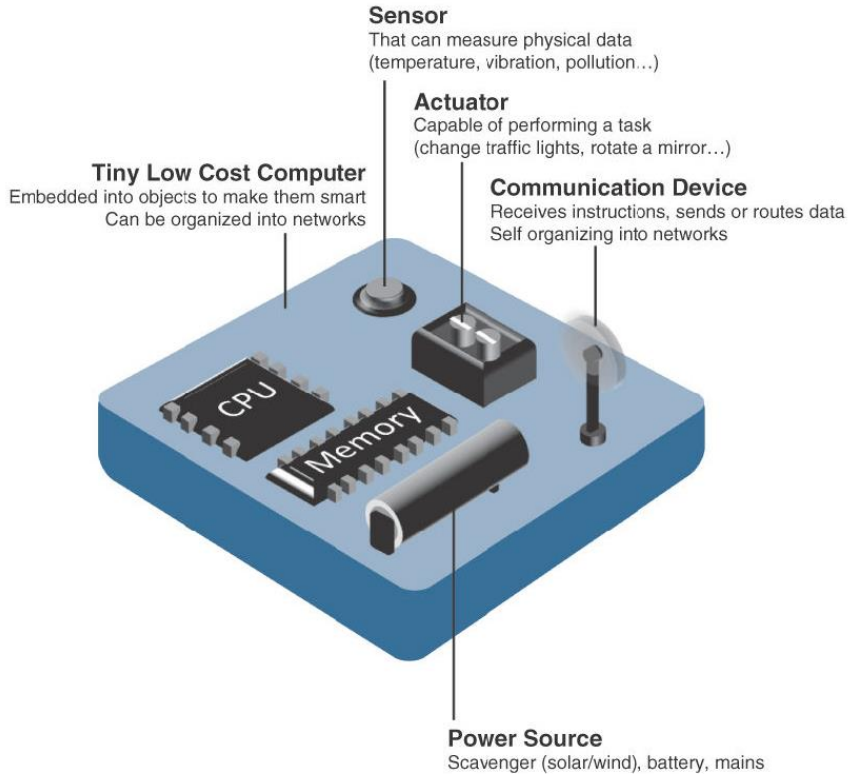

Events, insights, and actions are data flow and processing pipelines that occur across these structural parts.

# IoT Structural Components

**1. IoT Devices:** are the physical or virtual things that send events to and receive commands from IoT applications.

An IoT device has one or more of the following characteristics:

- ❑ Possesses a unique identity that distinguishes it within the solution.
- ❑ Has properties, or a state, that applications can access.
- ❑ Sends events to the IoT platform for applications to act on.
- ❑ Receives commands from applications to execute.

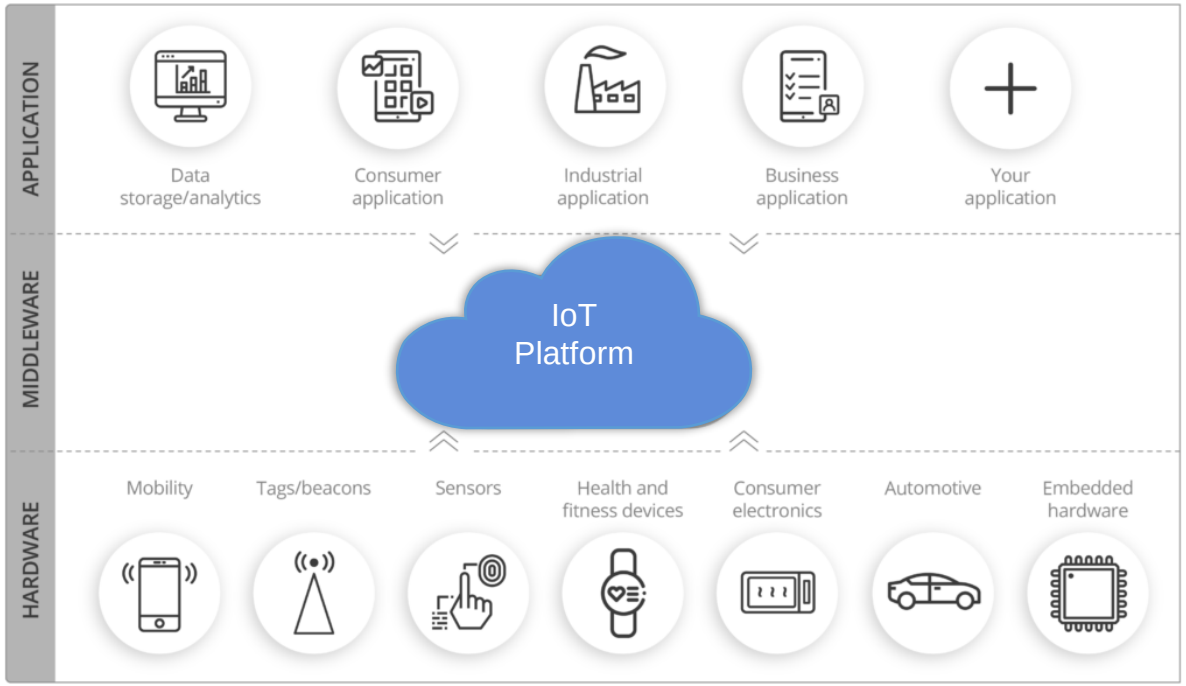


# IoT Structural Components

**2. IoT Platform:** is the collection of services that allow devices and applications to connect and communicate with each other.

The IoT platform at least:

- ❑ Brokers secure connectivity, authentication, and communication between devices and trusted applications.
- ❑ Generates contextual insights on incoming events to determine the routing of events to endpoints.



# IoT Structural Components

**3. Applications:** are the collection of scenario-specific services and components that are unique to an IoT solution.

IoT applications typically have:

- ❑ A mix of services for compute, storage, and event endpoints, combined with unique application business logic.
- ❑ Event workflows to receive and process incoming device events.
- ❑ Action workflows to send commands to devices or other processes.

# Connect IoT Devices to Platform

Connecting IoT devices to the IoT platform involves the following three processes:

**Attestation**

The attestation mechanism represents the method chosen for a device to confirm its identity when it connects to an IoT platform service.

**Authentication**

Authentication is how the device identifies itself. IoT platforms grant access to a device based on the device's ability to prove itself using its unique device identity in combination with its attestation mechanism.

**Provisioning**

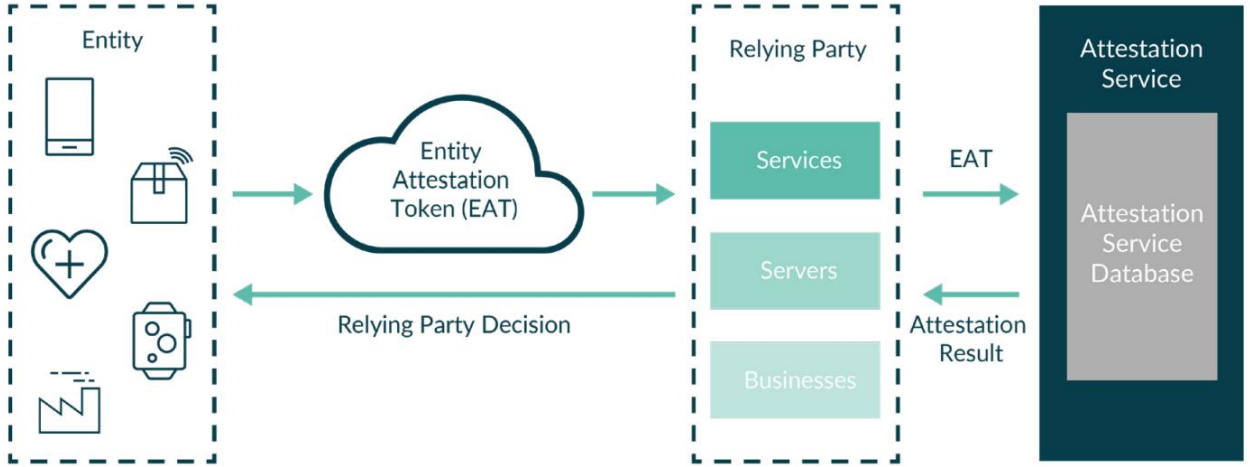
Provisioning is the act of enrolling a device into the IoT platform. Provisioning makes the platform aware of the device and the attestation mechanism the device uses.

# Connect IoT Devices to Platform

## Attestation

- The goal of attestation is to provide information about the device to other parties using a very simple, cryptographically secured token. Each information item in this token in known as a claim.

- The Attestation Service could be operated by the chip/device manufacturer, a third-party Attestation Service Provider, or a CSP.



# Connect IoT Devices to Platform

## Attestation

- An Entity Attestation Token (EAT) provides a signed (attested) set of claims that describe state and characteristics of an IoT device.
- These claims are used by a Relying Party to determine how much it wishes to trust the entity.

| Claim Name | Claim Description |
|---|---|
| Unique identifier | Similar to a serial number. Universally and globally identifies each individual device. |
| Manufacturer and model | Identifies the manufacturer of the chip and/or the finished device. |
| Installed software | Lists the software present on the device including versions. |
| Device boot and debug state | Indicates if the device booted securely, whether debug mode is enabled, and debug ports disabled. |
| Geographic position location | For example, based on GPS, WiFi, cell tower or some combination. Only available if the device has location features. |
| Versions, measurements and/ or integrity checks of running software | Measurements of running software, usually hashes of the code, are provided for comparison against known-good-value to help detect tampering. |
| Nonce | Cryptographic quality random number generated, sent by the server and returned as a claim to prevent replay and reuse. |

# Connect IoT Devices to Platform

## Authentication

- In order for a device or user to be authorized to access resources, it first needs to be properly authenticated or identified to the system.
- If the IoT device and the server are not identified properly it means that you cannot trust the data.

# Connect IoT Devices to Platform

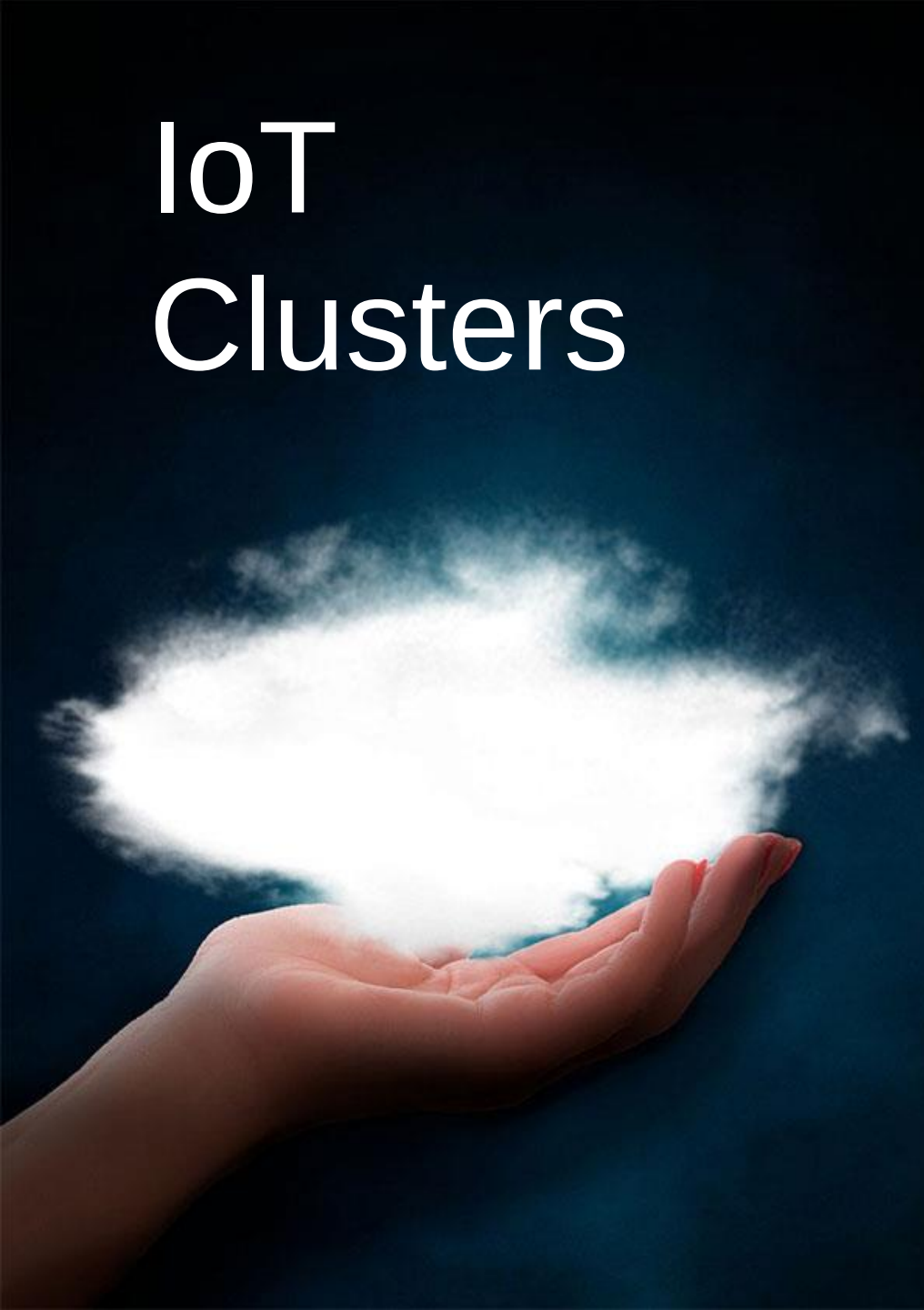
## Provisioning

In the context of provisioning IoT devices to their cloud solution, provisioning is a two part process:

1.Establishing the initial connection between the device and the IoT solution by registering the device.

2. Applying the proper configuration to the device based on the specific requirements of the solution it was registered to.

# IoT Clusters



## Verticals

- Indicate the use of IoT in a specific industry segment.
- Have unique regulatory bodies, supports specific standards, policies, procedures and protocols.

## Use cases

- Are served by the same platform and they usually need similar processing, storing, analyzing of data.

## Applications

- Use similar solutions and software

# IoT Verticals

## Industry

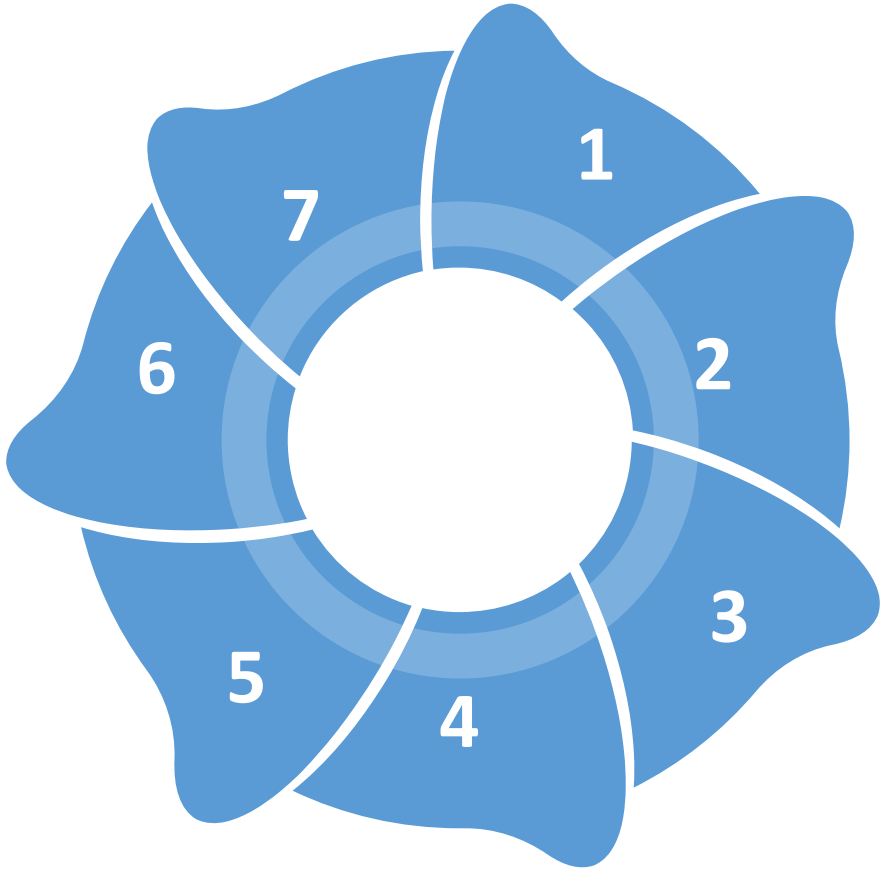
Reduce human error, improve process accuracy, and reduce overall operational costs.
**Use case:** smart factory, retail

## Smart home

Enhance the home experience by increasing security and automating home systems.
**Use cases:** smart kitchen

## Healthcare

Increase data driven decisions in both business matters and patient care.
**Use cases:** Health monitoring, activity recognition, safety.




## Energy

Eliminate on-site visits and increase regulatory compliance, reliability and efficiency.
**Use cases:** Smart grid, oil & gas, smart meters.

## Transportation

Enhance in-transit visibility while accelerating delivery time and operational efficiency.
**Use cases:** Connected vehicle, asset tracking

## Agriculture

Increase crop productivity through more efficient, environment-friendly processes.
**Use cases:** smart irrigation, Farm to fork

## Smart City

Interconnect all aspects of a city to improve citizen experience, safety and convenience factors.
**Use cases:** Smart street lighting, Environment monitoring.

# Risks and Challenges

**Security & Privacy**

More things becoming connected with other things and people. How individuals and businesses can control whether the collected data is shared and with whom.

**Interoperability**

Various protocols, architectures based on proprietary elements.

**Regulatory & Legal**

Businesses need to comply with various data protection, privacy and cybersecurity regulations

**Scalability**

Massive IoT to scale networks into the millions of devices.

**Big Data & Analytics**

How to evaluate massive amount of data arriving from different sources in various forms in a timely manner.


Thank You