Radio Frequency Identification

RFID is a form of wireless communication that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal or person. It uses radio frequency to search,identify, track and communicate with items and people. it is a method that is used to track or identify an object by radio transmission uses over the web. Data digitally encoded in an RFID tag which might be read by the reader. This device work as a tag or label during which data read from tags that are stored in the database through the reader as compared to traditional barcodes and QR codes.

Working of RFID System :

Every RFID system consists of three components: a scanning antenna, a transceiver and a transponder. When the scanning antenna and transceiver are combined, they are referred to as an RFID reader or interrogator. There are two types of RFID readers — fixed readers and mobile readers. The RFID reader is a network-connected device that can be portable or permanently attached. It uses radio waves to transmit signals that activate the tag. Once activated, the tag sends a wave back to the antenna, where it is translated into data.

The transponder is in the RFID tag itself. The read range for RFID tags varies based on factors including the type of tag, type of reader, RFID frequency and interference in the surrounding environment or from other RFID tags and readers. Tags that have a stronger power source also have a longer read range.

Differences between RFID and IoT

- IoT can support any network, while RFID requires a specific radio technology.
- IoT can work over short-, medium- and long-range networks, while RFID only works over a few inches or feet.
- IoT can support any kind of data communications, while RFID is only suited for brief tags or authentication tokens.
- IoT is better for capturing real-time sensor data, while RFID is better suited for recording objects' proximity.
- IoT devices tend to be more complex and expensive, while RFID tags are generally optimized for low cost and simplicity.
- IoT can exchange data across wireless and wired networks, while RFID reads data in one direction from nearby tags.
- In addition, less common types of RFID with more expensive active tags can support longer ranges and two-way communication in some use cases.

How RFID and IoT can work together

RFID and IoT are complementary technologies that users frequently combine.RFID provides dependable connectivity between physical products and RFID readers that are connected to the internet. Most of these implementations take advantage of IoT capabilities for sharing data between physical devices and cloud databases to support various authentication, transaction, analytics and control use cases. Users can sometimes combine these with other technologies such as barcode tags and readers, which can be more cost-effective in some scenarios.

WIRELESS SENSOR NETWORK IN IOT

Wireless Sensor Network in IoT is an infrastructure-less wireless network that is used for deploying a large number of wireless sensors that monitor the system, physical and environmental conditions. Our extremely motivated and professional engineers are very well equipped to provide you with an all round solution if you are looking to incorporate WSN in your business.

NETWORKS CONNECTING WIRELESS SENSORS

To connect Sensors embedded in IoT devices, a communication protocol is used. A low-power wide-area network ,LPWAN, is a type of wireless network designed to allow long-range communications between these IoT devices.Lora based Wireless Sensor network is widely used. Sub-1 GHz, Zigbee,Thread etc are also used to connect sensor networks and gateway and data collected from this sensor network can be sent to cloud using cellular networks such as NBIoT, LTE-M or wifi etc.

WIRELESS SENSOR NETWORK APPLICATIONS

Patient monitoring in hospitals ,

Home security,

Military applications,

Livestock monitoring ,

Server Room monitoring

Wireless sensor network for smart agriculture

Wireless sensor network for forest fire detection

Wireless sensor network for water quality monitoring

Wireless sensor network for office monitoring

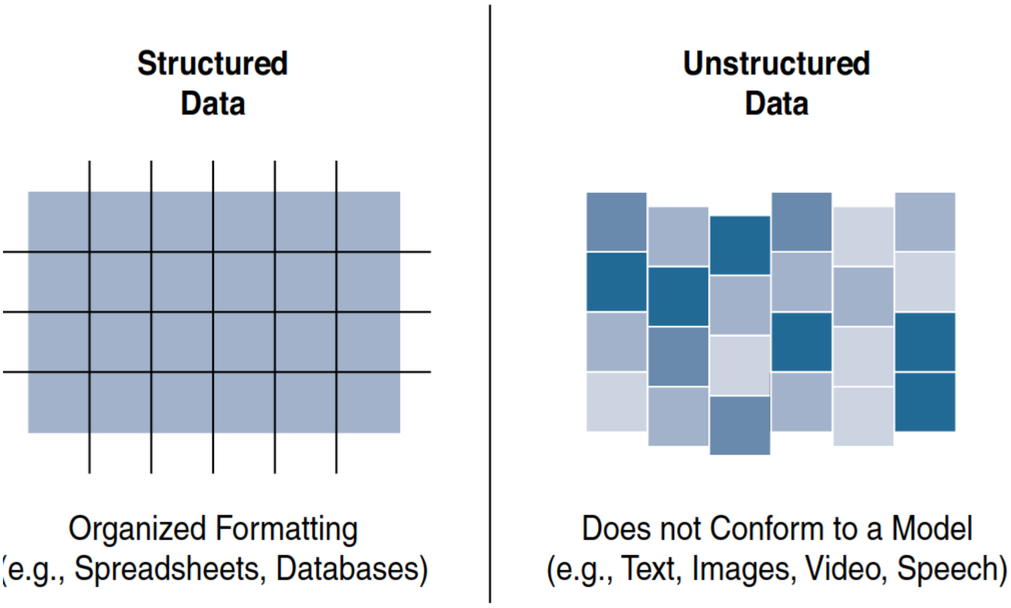
Wireless sensor network for environmental monitoring

Wireless sensor network for landslide detection

Wireless sensor network for IoT security

BigData Analytics

Structured data and unstructured data are important classifications as they typically require different toolsets from a data analytics perspective. Figure 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).

Structured data can be found in most computing systems and includes everything from banking transaction and invoices to computer log files and router configurations. IoT sensor data often uses structured values, such as temperature, pressure, humidity, and so on, which are all sent in a known format. Structured data is easily formatted, stored, queried, and processed; for these reasons, it has been the core type of data used for making business decisions.

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.2 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.

With machine learning applications, such as natural language processing (NLP), you can decode speech. With image/facial recognition applications, you can extract critical information from still images and video.

IoT Data Analytics Overview

The true importance of IoT data from smart objects is realized only when the analysis of the data leads to actionable business intelligence and insights. Data analysis is typically broken down by the types of results that are produced.

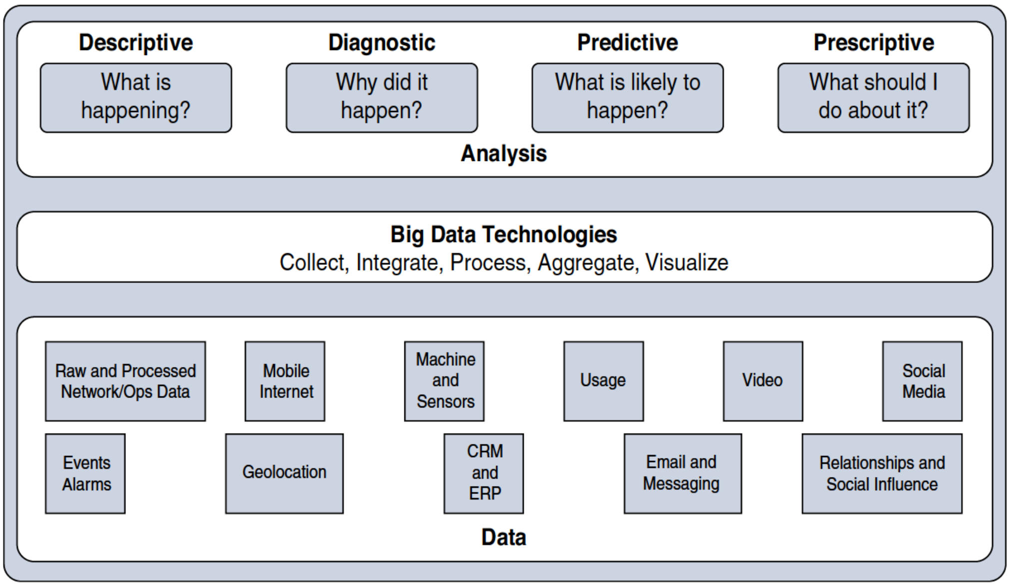


Fig: Types of Data Analysis Results

- **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.

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 data- base 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 Computing

Cloud Internet of Things (IoT) uses cloud computing services to collect and process data from IoT devices, and to manage the devices remotely. The scalability of cloud IoT platforms enables the processing of large amounts of data, as well as artificial intelligence (AI) and analytics capabilities.

Cloud IoT is a technology architecture that connects IoT devices to servers housed in cloud data centers. This enables real-time data analytics, allowing better, information-driven decision making, optimization, and risk mitigation. Cloud IoT also simplifies management of connected devices at-scale.

Cloud IoT is different from traditional, or non-cloud-based IoT in a few key ways:

- **Data Storage:** the cloud collects IoT data generated by thousands or millions of IoT sensors, with the data being stored and processed in a central location. While in other types of IoT architectures, data may be stored and processed on-premises
- **Scalability:** cloud IoT is highly scalable, as cloud infrastructure (compute, storage, and networking resources) can easily handle thousands of devices and process their data across large systems
- **Flexibility:** cloud IoT provides a high level of flexibility, as it allows devices to be added or removed as-needed, without having to reconfigure the entire system

- **Maintenance:** in cloud IoT, the maintenance of servers and networking equipment is handled by the cloud service provider (CSP). While in other types of IoT architectures, maintenance may be the responsibility of the end user
- **Cost:** cloud IoT can be more cost-effective over the long-term, as users only pay for the resources they actually consume, and users do not have to invest upfront in their own expensive compute, storage, and networking infrastructure

Cloud IoT connects IoT devices – ***which collect and transmit data*** – to cloud-based servers via communication protocols such as MQTT and HTTP and over wired and wireless networks. These IoT devices can be managed and controlled remotely and integrated with other cloud services.

IoT data is sourced from anywhere and everywhere, including sensors, actuators, operating systems, mobile devices, standalone applications, and analytic systems. By involving the cloud, vast amounts of IoT data can be stored and processed in a central location.

A cloud IoT system typically includes the following elements:

- **IoT Devices:** physical devices, such as sensors and actuators, that generate and transmit data to the cloud
- **Connectivity:** communication protocols and standards used to connect the IoT devices to the cloud. Examples of protocols include MQTT and HTTP, while examples of standards are Wi-Fi, 4G/LTE, 5G, Zigbee, and LoRa (long range)
- **Cloud Platforms:** cloud service providers (CSPs) that offer infrastructure and services to connect to the IoT devices. Examples include AWS IoT and Azure IoT
- **Data Storage:** cloud-based storage for data generated by the IoT devices, which can be housed in repositories such as a database, data warehouse, or data lake
- **Application Layer or API:** cloud IoT platforms typically provide a native application – *for analytics, machine learning (ML), and visualization* – or application programming interface (API) – *for data processing*. Usually, applications offer the ability to manage and monitor the IoT devices for provisioning, software updates, and troubleshooting
- **Security:** measures put in place to secure the data and IoT devices, such as encryption, authentication, and access control

Example – Cloud and IoT System

To illustrate all of the above elements in action, consider the example of a wind farm. A typical wind turbine can have about 108 sensors, and the average wind farm houses roughly 150 turbines, for a total of over 16,000 sensors. The data from these sensors might be sent to the cloud for storage, via 5G cellular broadband.

Once the data is stored on cloud servers, it can be used to monitor wind turbine performance, track turbine health, and adjust operating parameters as needed. Cloud IoT platforms also help with predictive maintenance, which is useful given that wind turbines on such a wind farm would be spread across an area of over 15 square miles (39 square kilometers), and downtime could result in millions of dollars of losses per year.

What are the Cloud Services for IoT?

Cloud platforms deliver a collection of capabilities that allow Internet of Things (IoT) devices to interact with cloud services, other applications, and even other IoT devices. These cloud platforms let users centrally onboard, manage, monitor, and control IoT devices.

In addition, the cloud supports services such as scalable storage, device connectivity, analytics and reporting, and identity and access management (IAM) in IoT.

Scalable Storage

Cloud IoT platforms provide scalable object storage services, such as Amazon Simple Storage Service (Amazon S3), that allow organizations to easily increase or decrease their data storage requirements. This type of flexibility is beneficial for IoT applications, as they often generate large volumes of unstructured data and must be able to store this information without sacrificing device performance.

Device Connectivity

Cloud-based IoT platforms offer straightforward, reliable, and secure connectivity at-scale between physical IoT devices and cloud services. In turn, an organization can connect thousands or millions of IoT devices to the cloud, without the need to provision or manage the requisite servers and networking equipment.

Analytics and Reporting

Cloud-based IoT platforms are equipped with powerful analytics capabilities – *in combination with computing resources* – that enable organizations to gain real-time insights into the large datasets that IoT devices produce. Through sophisticated algorithms, such as predictive modeling, statistical analysis, and machine learning (ML), IoT device data can be used to improve efficiency and make better, information-driven decisions.

Identity and Access Management (IAM)

Security for the data generated by IoT devices can be protected in the cloud using Identity and Access Management (IAM), which is an authentication and authorization service. IAM enables organizations to grant or deny access to services and resources in the cloud for large numbers of users with different access needs.