1.protocol standardization of iot

**Most common protocols**

Technologists can select from multiple communication protocols when building a network to serve their IoT ecosystem. The most common include the following.

**1. AMQP**

Short for Advanced Message Queuing Protocol, AMQP is an open standard protocol used for more message-oriented middleware. As such, it enables messaging interoperability between systems, regardless of the message brokers or platforms being used. It offers security and interoperability, as well as reliability, even at a distance or over poor networks. It supports communications, even when systems aren't simultaneously available.

**2. Bluetooth and BLE**

Bluetooth is a short-range wireless technology that uses short-wavelength, ultrahigh-frequency radio waves. It had most commonly been used for audio streaming, but it has also become a significant enabler of wireless and connected devices. As a result, this low-power, low-range connectivity option is a go-to for both personal area networks and IoT deployments.

Another option is [Bluetooth Low Energy](https://www.techtarget.com/iotagenda/definition/Bluetooth-Low-Energy-Bluetooth-LE), known as either Bluetooth LE or BLE, which is a new version optimized for IoT connections. True to its name, BLE consumes less power than standard Bluetooth, which makes it particularly appealing in many use cases, such as health and fitness trackers and smart home devices on the consumer side and for in-store navigation on the commercial side.

**3. Cellular**

Cellular is one of the most widely available and well-known options available for IoT applications, and it is one of the best options for deployments where communications range over longer distances. Although 2G and 3G legacy cellular standards are now being phased out, telecommunications companies are rapidly expanding the reach of newer high-speed standards -- namely, 4G/LTE and 5G. Cellular provides high bandwidth and reliable communication. It's capable of sending high quantities of data, which is an important capability for many IoT deployments. However, those features come at a price: higher cost and power consumption than other options.

**4. CoAP**

The Internet Engineering Task Force Constrained RESTful Environments Working Group in 2013 launched CoAP, for Constrained Application Protocol, having designed it to work with HTTP-based IoT systems. CoAP relies on User Datagram Protocol to establish secure communications and enable data transmission between multiple points. Often used for machine-to-machine ([M2M](https://www.techtarget.com/iotagenda/definition/machine-to-machine-M2M)) applications, CoAP enables constrained devices to join an IoT environment, even with the presence of low bandwidth, low availability and/or low-energy devices.

**5. DDS**

Object Management Group (OMG) developed Data Distribution Service for real-time systems. OMG describes DDS as "a middleware protocol and API standard for data-centric connectivity," explaining that "it integrates the components of a system together, providing low-latency data connectivity, extreme reliability and a scalable architecture that business and mission-critical IoT applications need." This M2M standard enables high-performance and highly scalable real-time data exchange using a publish-subscribe pattern.

**6. LoRa and LoRaWAN**

LoRa, for long range, is a noncellular wireless technology that, as its name describes, offers long-range communication capabilities. It's low power with secure data transmission for M2M applications and IoT deployments. A proprietary technology, it's now part of Semtech's radio frequency platform. The LoRa Alliance, of which Semtech was a founding member, is now the governing body of LoRa technology. The LoRa Alliance [also designed and now maintains LoRaWAN](https://www.techtarget.com/searchnetworking/answer/What-is-the-difference-between-LoRa-and-LoRaWAN), an open cloud-based protocol that enables IoT devices to communicate LoRa.

**7. LWM2M**

OMA SpecWorks describes its Lightweight M2M (LWM2M) as "a device management protocol designed for sensor networks and the demands of an M2M environment." This communication protocol was designed specifically for remote device management and telemetry in IoT environments and other M2M applications; as such, it's a good option for low-power devices with limited processing and storage capabilities.

**8. MQTT**

Developed in 1999 and first known as Message Queuing Telemetry Transport, it's now just MQTT. There is no longer any message queueing in this protocol. MQTT uses a publish-subscribe architecture to enable M2M communication. Its simple messaging protocol works with constrained devices and enables communication between multiple devices. It was designed to work in low-bandwidth situations, such as for sensors and mobile devices on unreliable networks. That capability makes it a commonly preferred option for connecting devices with a small code footprint, as well as for wireless networks with varying levels of latency stemming from bandwidth constraints or unreliable connections. MQTT, which started as a proprietary protocol, is now the leading open source protocol for connecting IoT and [industrial IoT](https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT) devices.

**9. Wi-Fi**

Given its pervasiveness in home, commercial and industrial buildings, Wi-Fi is a frequently used IoT protocol. It offers fast data transfer and is capable of processing large amounts of data. Wi-Fi is particularly well suited within LAN environments, with short- to medium-range distances. Moreover, Wi-Fi's multiple standards -- the most common in homes and some businesses being 802.11n -- give technologists options for deployment. However, many Wi-Fi standards, including the one commonly used in homes, is too power-consuming for some IoT use cases, particularly low-power/battery-powered devices. That limits Wi-Fi as an option for some deployments. Additionally, Wi-Fi's low range and low scalability also limit its feasibility for use in many IoT deployments.

**10. XMPP**

Dating back to the early 2000s when the Jabber open source community first designed its Extensible Messaging and Presence Protocol for real-time human-to-human communication, [XMPP is now used for M2M communication](https://www.techtarget.com/iotagenda/feature/XMPP-IoT-protocol-winner-or-second-place-to-MQTT) in lightweight middleware and for routing XML data. XMPP supports the real-time exchange of structured but extensible data between multiple entities on a network, and it's most often used for consumer-oriented IoT deployments, such as smart appliances. It's an open source protocol supported by the XMPP Standards Foundation.

**11. Zigbee**

Zigbee is a mesh network protocol that was designed for building and home automation applications, and it's one of the most popular mesh protocols in IoT environments. A short-range and low-power protocol, Zigbee can be used to extend communication over multiple devices. It has a longer range than BLE, but it has a lower data rate than BLE. Overseen by the Zigbee Alliance, it offers a flexible, self-organizing mesh, ultralow power and a library of applications.

**12. Z-Wave**

Another proprietary option, Z-Wave is a wireless mesh network communication protocol built on low-power radio frequency technology. Like Bluetooth and Wi-Fi, Z-Wave lets smart devices communicate with encryption, thereby providing a level of security to the IoT deployment. [It's commonly used for home automation products](https://www.techtarget.com/iotagenda/blog/IoT-Agenda/New-revenue-streams-abound-as-connected-homes-accelerate) and security systems, as well as in commercial applications, such as energy management technologies. It operates on 908.42 MHz radio frequency in the U.S.; although, its frequencies vary country by country. Z-Wave is supported by the Z-Wave Alliance, a member consortium focused on expanding the technology and interoperability of devices that use Z-Wave.

## **5]What are the security issues in the IoT?**

While IoT devices play a huge role in the discussion of IoT security, placing all the focus on this aspect of the IoT does not provide a full picture of why security is necessary and what it entails. There are many factors that make IoT security critical today.

**Threats and risks**

IoT security is critical largely because of the expanded [attack surface](https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/the-iot-attack-surface-threats-and-security-solutions) of threats that have already been plaguing networks. Adding to these threats are insecure practices among users and organizations who may not have the resources or the knowledge to best protect their IoT ecosystems.

These security issues include the following:

* **Vulnerabilities.**Vulnerabilities are a large problem that constantly plague users and organizations. One of the [main reasons IoT devices are vulnerable](https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/smart-yet-flawed-iot-device-vulnerabilities-explained) is because they lack the computational capacity for built-in security. Another reason that vulnerabilities can be so pervasive is the limited budget for developing and testing secure firmware, which is influenced by the price point of devices and their very short development cycle. Vulnerable standard components also affect millions of devices, as demonstrated by [Ripple20](https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/millions-of-iot-devices-affected-by-ripple20-vulnerabilities) and [URGENT/11](https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/fda-warns-against-urgent-11-vulnerabilities-affecting-medical-devices-and-hospital-networks). Aside from the devices themselves, vulnerabilities in web applications and related software for IoT devices can lead to compromised systems. Malware operators are on the lookout for such opportunities and are knowledgeable even about older vulnerabilities.
* **Malware.**Despite the limited computing capacity of most IoT devices, they can still be infected by malware. This is something cybercriminals have used to great effect in the past few years. [IoT botnet malware](https://www.trendmicro.com/vinfo/us/security/definition/iot-botnet) are among the most frequently seen variants, as they are both versatile and profitable for cybercriminals. The most notable attack was in 2016, when [Mirai took down major websites and services](https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet) using an army of ordinary IoT devices. Other malware families include [cryptocurrency mining malware](https://www.trendmicro.com/en_us/research/18/e/cryptocurrency-mining-malware-targeting-iot-being-offered-in-the-underground.html) and ransomware.
* **Escalated cyberattacks.**Infected devices are often used for distributed-denial-of-service (DDoS) attacks. Hijacked devices can also be used as an attack base to infect more machines and mask malicious activity, or as an entry point for lateral movement in a corporate network. While organizations may seem like the more profitable targets, smart homes also see [a surprising number of unforeseen cyberattacks](https://www.infosecurity-magazine.com/news/smart-home-experiences-cyber/).
* **Information theft and unknown exposure.** As with anything dealing with the internet, connected devices increase the chances of exposure online. Important technical and even personal information can be unknowingly stored and targeted in these devices.
* **Device mismanagement and misconfiguration.** Security oversights, poor password hygiene, and overall device mismanagement can assist in the success of these threats. Users may also simply lack the knowledge and the capability to implement proper security measures, wherein service providers and manufacturers may need to help their customers achieve better protection.

**Emerging issues**

The lack of industry foresight gave little time to develop strategies and defenses against familiar threats in growing IoT ecosystems. Anticipating emerging issues is one of the reasons research on IoT security must be done continuously. Here are some of the emerging issues that need to be monitored:

* **Complex environments.**In 2020, most U.S. households had access to an average of [10 connected devices](https://www.statista.com/statistics/1107206/average-number-of-connected-devices-us-house/). This research paper defined [complex IoT environments](https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/threats-and-risks-to-complex-iot-environments) as an interconnected web of at least 10 IoT devices. Such an environment is nearly impossible for people to oversee and control because of its elaborate web of interconnected functions. An overlooked misconfiguration in such a scenario can have dire consequences and even put the physical household security at risk.
* **Prevalence of remote work arrangements.**The Covid-19 pandemic has usurped many expectations for the year 2020. It brought about large-scale work-from-home (WFH) arrangements for organizations around the globe and pushed heavier reliance on home networks. IoT devices also proved useful for many users’ WHF setups. These changes have highlighted the need to reexamine IoT security practices.
* **5G connectivity.**The transition to 5G comes with much anticipation and expectations. It is a development that will also enable other technologies to evolve. At present, much of the research on 5G remains largely focused on how it will affect enterprises and how they can [implement it securely](https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/the-transition-to-5g-security-implications-of-campus-networks).

**The possible consequences of IoT attacks**

Aside from the threats themselves, their consequences in the context of the IoT can be much more damaging to deal with. The IoT has the unique capability of affecting both virtual and physical systems. Cyberattacks on IoT ecosystems could have far more unpredictable effects because they translate more easily into physical consequences. This is most prominent in the field of [industrial internet of things (IIoT)](https://www.trendmicro.com/vinfo/us/security/definition/industrial-internet-of-things-iiot), where [past cyberattacks](https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-the-industrial-internet-of-things-addressing-iiot-risks-in-healthcare) had already demonstrated cascading consequences. In [the healthcare industry](https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-the-industrial-internet-of-things-addressing-iiot-risks-in-healthcare), IoT devices are already being utilized to remotely monitor patients’ vital signs and has proven very [helpful during the pandemic.](https://iottechnews.com/news/2021/jul/12/turning-to-iot-for-better-patient-care-beyond-the-pandemic/) Attacks on such devices can expose sensitive patient information or even endanger their health and safety. In the smart home, [exposed devices](https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/inside-the-smart-home-iot-device-threats-and-attack-scenarios) could allow cybercriminals to monitor the household, compromise security devices like smart locks, and turn devices against their owners, as was the case when a [baby monitor](https://www.iotforall.com/baby-monitor-hackers) and a [smart thermostat](https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hacker-compromised-family-s-wi-fi-taunted-family-with-thermostat-camera-for-24-hours) were hacked in separate attacks.

6)

# Introduction to Unified Data

Unified data is when a company merges its many fragmented data sources into one, single central view. Unified data provides a more complete and accurate picture of a company’s data, but unifying the data is far from simple. To tie data sources together, companies need a system to unite them, such as an analytics platform.

### Why is unified data so great?

Companies strive to unify their data because, by default, most data is inaccessible. It’s often scattered throughout the company and divided into information silos among business units and teams. Without a central way to manage data, businesses can’t make informed decisions. Marketing teams can’t accurately measure demand for their product. Product teams can’t fully [understand their customer journey](https://mixpanel.com/blog/2017/10/31/insights-from-saas-product-experts/), and analytics teams, which are often tasked with breaking down information silos, can’t provide accurate business intelligence to leadership. When companies are able to unify their data, they make all of their business units more productive. But unifying data can pose a tremendous organizational challenge, as well as an engineering one.

### The challenge of creating unified data

The technologies that businesses use to store data are highly fragmented. There are tens of thousands of hardware and software providers that each have their own vernacular, programming languages, syntaxes, and practices. On-premise storage servers may not be able to speak to cloud-hosted business intelligence tools which can’t access virtualized servers. Conventions like application programming interfaces (APIs) can connect systems, but don’t always offer enough functionality. Additionally, not all data is the same. There’s [big data](https://mixpanel.com/blog/2018/02/22/story-roundup-data-science/), thick data, and structured, unstructured, and multi-structured data. Some systems can only process certain types of data, and each dataset can vary wildly. It is little wonder that [85 percent of companies](http://newvantage.com/wp-content/uploads/2017/01/Big-Data-Executive-Survey-2017-Executive-Summary.pdf) strive to be data-driven yet only 37 percent claim to be successful at using their data. Most data ecosystems rival the United Nations in complexity. Every application speaks slightly different dialects and they require translators to communicate. Businesses that succeed at unifying their data, are better able to plan, budget, forecast, and build products. For unification, many businesses turn to [analytics platforms](https://mixpanel.com/platform/).

### How can analytics platforms help with unified data?

Analytics platforms are purpose-built to capture, store, and analyze data from a variety of sources. They are, by definition, [tools for unifying data](https://mixpanel.com/platform/). Most offer pre-built integrations to common systems and universal APIs for less common ones. They allow enterprises to tie their ERP, CRM, web applications, marketing systems, customer applications, and data partners together to view the data from one interface. The best analytics platforms have highly intuitive interfaces that are designed to mask the complexity of the underlying data architecture. They use dashboards to help users visualize their data. Some platforms offer [machine learning algorithms](https://mixpanel.com/machine-learning/) to simplify and automate the process of analysis. Brands can use an analytics platform to knit data from across silos, business units, and teams together and provide everyone access. The more individuals within a business that are data-informed, the better. At e-signature provider DocuSign, the product team gave [over 100 individuals](https://mixpanel.com/customers/docusign-accelerates-growth/) across the business access to its Mixpanel instance so that the data science team wouldn’t serve as an insight bottleneck.

### How to create a unified data ecosystem

Analytics platforms each have their own quirks. Some are designed to be highly accessible but lack advanced features for manipulating data. Others are designed to handle massively complex datasets but suffer from what’s known as [featuritis](https://mixpanel.com/blog/2017/12/21/drive-b2b-engagement-with-marketing-psychology/" \t "_blank)–a confusing interface with too many features. Some platforms strike a balance of high functionality and high usability. When teams evaluate analytics platforms, they should find the one that best fits their current and future needs. **Teams can examine analytics platforms based on these factors:**

* **Integrations**: Can the platform integrate with most data sources?
* **Performance**: Does the platform have a high storage capacity?
* **Reliability**: Does the platform guarantee access?
* **Availability**: Does the platform guarantee uptime?
* **Latency**: Can users access data in near real-time?
* **Concurrency**: Can the platform use faster, non-relational query techniques?
* **Compliance**: Is the platform data center compliant?
* **Innovation**: Is the company constantly improving its product?

In addition to features, it’s important for teams to consider process issues like internal data governance and quality. Pieces of legislation like the European Union’s [GDPR](https://mixpanel.com/blog/2017/12/21/gdpr-mixpanel-readiness/) are forcing many companies into an era greater data transparency. Customers increasingly demand to know what data businesses collect on them, and what they use it for. Businesses need to ensure that they are being transparent with user data. At the same time, data breaches are increasingly common. Any teams seeking to unify their data must also consider the potential danger of making it easier for hackers to access. To keep themselves safe, teams can publish internal data governance guidelines and make sure their partners are compliant and can customer data secure.

-----------------------------------------------------------------------------------------

What is SCADA system? Learn About its Application in IoT Projects

In this article, our Industrial Automation and IoT developers have helped us understand various features of a SCADA system and what are its applications in Home and Industrial automation based IoT projects.

We will also share brief information about technologies, frameworks and platforms that power a fully-functional SCADA system.

What is a SCADA Software System? – An Introduction

SCADA stands for Supervisory Control And Data Acquisition.

SCADA software system is a device monitoring and controlling framework. The supervisory control includes, taking action and control through remote locations for various control mechanisms and processes.

Various kinds of data can be acquired from network of devious (connected through wireless/wired communication systems) for storage, processing and analytics to aid decision making.

Frontend of a SCADA software solution is a graphical user interface (GUI/UI).

In a nutshell, a SCADA software solution is a real time monitoring, supervision and control system from remote and/or local physical location.

How does The SCADA software system work:

SCADA Software

Let’s try to understand the functional blocks of a SCADA based IoT system, with the help of the simplified IoT framework as shown above

The User Interface(UI) of Mobile App or Web based dashboard represented above is the HMI of the SCADA system.

This, along with the backend business logic, database (cloud server) and a Gateway constitutes of a SCADA solution for control and monitoring of devices in an IoT network.

The IoT gateway ensures compatibility between IoT sensor network and cloud server. Through the gateway, the sensor data is stored in the cloud server.

The cloud server is the hosting spot for the algorithms that implement the business logic.

The sensor unit detects the change in the environment like change in temperature, sound and also acts as a data accumulating unit.

There can be a number of devices or machines connected within a SCADA solution based IoT project. For an instance, in case of home automation system, various home appliances such as AC, lights, refrigerator can be a part of connected smart home.

Hence SCADA solution is an intelligent software system with an intuitive UI (for data representation) connected with cloud server for data processing and predictive and descriptive analysis.

Let us see the detailed features of a SCADA software system

Features Supported by SCADA:

System Management Features:

The interactive user interface of the SCADA system has evolved over a period of time.It includes graphical representation of the whole system, showing data in a consolidated manner.

Typically a SCADA solution will support following two types of system management features:

Device Management: The number of nodes or devices being monitored or maintained is visible from the UI and can be subcategorized further into different parameters.

For instance, in case of industrial automation, the control units installed in a particular production floor can be categorized under geographical location and admin level of that particular system.

Also an overview of the whole production floor can be seen, with the total number of such control units installed. The number of devices installed, depend on the type of network topology used.

User Management: The permission and roles can be defined under user management panel with respect to the level of users. The specific admin roles can be assigned and limited access to other level of user for various data and for the interface as well, can be imposed.

Device and System Control Features:

In the SCADA system, both remote and local access is prevalent and ranges widely on the basis of the users and industries for which the application has been built.It is interesting to take into consideration that SCADA software has the intelligence to recognize the different communication signals of different devices installed.

For example, let us consider the home automation system, the doors are automated using proximity sensors but the AC communicates with the IR sensor technology. SCADA can be designed to ensure compatibility.The interoperability is ensured by the IoT gateways that are part of the SCADA system architecture.

Another important feature of Control mechanism is system failure management. The SCADA system has defined algorithms and business logic to trigger a specific alert in case of any gateway or device failure.

Here the question of data loss arises, which again is meticulously handled by the SCADA software system. The signal containing packets of data does not get lost in case of data failure but simply stored in the memory, pipelined for immediate communication when the health of the device or gateway is redeemed.

One queer and interesting aspect in SCADA software is IFTTT (if this then that). This special method of logical looping gives the user a control in the interface of the UI for better handling or option of a changed maneuver of the series of operations.

There are various logics that can be customized to control the pattern of data flow. The SCADA on a large scale is able to do the parallel processing of a large data simultaneously.

This is an utmost important feature w.r.t industrial automation application where bulk processing is needed. Also the logics can be altered depending on the business need and the pattern of flow can be modifies if and when required.

Monitoring Features:

The inevitable benefit of SCADA based system comes into play while performance optimization. Data is available both in structured and unstructured format and can be recognised and processed efficiently by the SCADA system. There are two types of data analytics that SCADA supports:

Descriptive Analytics:The descriptive analysis of data gives the user a proper idea of comparative efficiency on genuine parameters of a particular device.For instance, from the business perspective the decision making on what services to use or how to generate revenue or propel business is based on analysis of past data of the quality of services provided and the outcome.This process is known as judgement analytics and it is based on pattern recognition of the adaptive behavior intelligence of SCADA

Predictive Analytics:The future or predictive analysis of a system are logical algorithms to analyze the past data and generate a predictive alert in case of any threats or anticipated failure in case of devices.This area is yet under speculative research and development which has a large prospect of implementation, in scope of various manufacturing industries. The medical industry has been using the predictive analysis of data for effective treatment methodologies.

Support for automated and customized reporting:User defined reports can be synthesized using backend programming. Automated reports are mainly a health check of a particular functionality which can be generated in form of automated mailer alerts or specific admin alerts. This feature also helps in data acquisition and analysis in terms of user or industry admin operation and maintenance of a functional module.

What is RFID and how does it work?

Radio Frequency Identification – or RFID – is used to automatically identify an object and capturing data about that object that has been stored in a small microchip tag and attached to the object. The RFID tag has a built-in antenna that communicates to a scanning device that reads the data remotely. The data is then transferred from the scanning device to the enterprise application software that houses the data. Each RFID tag has its own unique identifying number.

RFID can be used to record and control the movement of assets and personnel. You’ve probably seen RFID tags on the back of your library books, or even in the new biometric passports. It makes tracking assets contained in boxes or pallets easier to manage.

The components of RFID

Using radio waves and electromagnetic fields to send data, an RFID tag and the system that reads it consists of three main components.

Component #1 – the RFID tag: there are two types of RFID tags, passive and active. A passive RFID tag is the barcode you see in the supermarket. It is assigned to an item, it is easy to activate, and it does not have a power supply. An active RFID tag, like the sensor tag in the back of a library book, has a microchip that collects information about the asset and may also contain an antenna or on-board sensor.

Component #2 – the RFID reader: An RFID reader is a device that scans the RFID tag and collects information about the asset the tag is attached to. These readers can be hand-held or wired, and work with USB and Bluetooth. Not all barcode scanners can read an RFID tag, but all RFID readers can read a barcode.

Component #3 – the RFID applications or software: this software controls and monitors the RFID tags that have been attached to your assets. It can be a mobile application or a standard software package. Most of the time you can find RFID software that has a mobile application that works in conjunction with it. This software can communicate with the reader using Bluetooth or Beacon technology.

How Are RFID Used with IoT Devices?

When used in IoT, RFID tags are handy in cameras, GPS, and other smart sensors. Thy can help identify and locate objects. It is an inexpensive way to turn objects in the home “smart,” like the popular line of Google Nest products. Some healthcare systems are using RFID tags to track patients and their medical records. Transportation systems are using RFID to read passenger data, keep traffic in control, and update transport systems.