SUMATOSOFT

IoT Ecosystem: Top 7 Components

sumatosoft.com
info@sumatosoft.com

One Boston Place, Suite 2602 Boston, MA 02108, United States

How Ecosystems Look and What Lies Behind the Term IoT Ecosystem

The Internet of Things concept became quite a discussable topic in recent years. Google trends show that people have a constant interest in the term “IoT” in recent years. The interest over time rate stays at 26 points on average over the 2022 year, reaching 86 at its peaks. According to McKinsey Digital insights, 127 devices were hooking up to the internet for the first time every second in 2020. And 173 million smartwatches were shipped in 2022.

Everything is related to everything else.

When discussing any ecosystem, we’re essentially talking about a sophisticated network of interconnected components and the environment they inhabit. These elements are tied together through various conduits such as energy flows or cycles—much like nutrient cycles in biological systems. What sets an ecosystem apart from a mere system is this crucial intersection with the environment. While a system forms a unified, albeit complex whole, an ecosystem is deeply intertwined with the environment it exists in.

The term “IoT Ecosystem” is more fitting than “IoT System” because IoT devices derive their value from the context in which they operate. Their primary contribution is the data they generate, data that often relates to environmental conditions or external phenomena, as well as internal system metrics. In addition to their environmental interactions, these devices are also interconnected, sharing data and functionality. Ultimately, the end-user of this complex web of data is the human operator, who leverages it for various purposes.

The main benefit IoT devices bring to people is the data.

These three facts (environment, data, people) bring us to the definition of an Internet of Things ecosystem – a network of interconnected devices that exists in some environment gathers the data and delivers it to people who process and analyze it using modern technologies to achieve a definite goal like building a smart home.

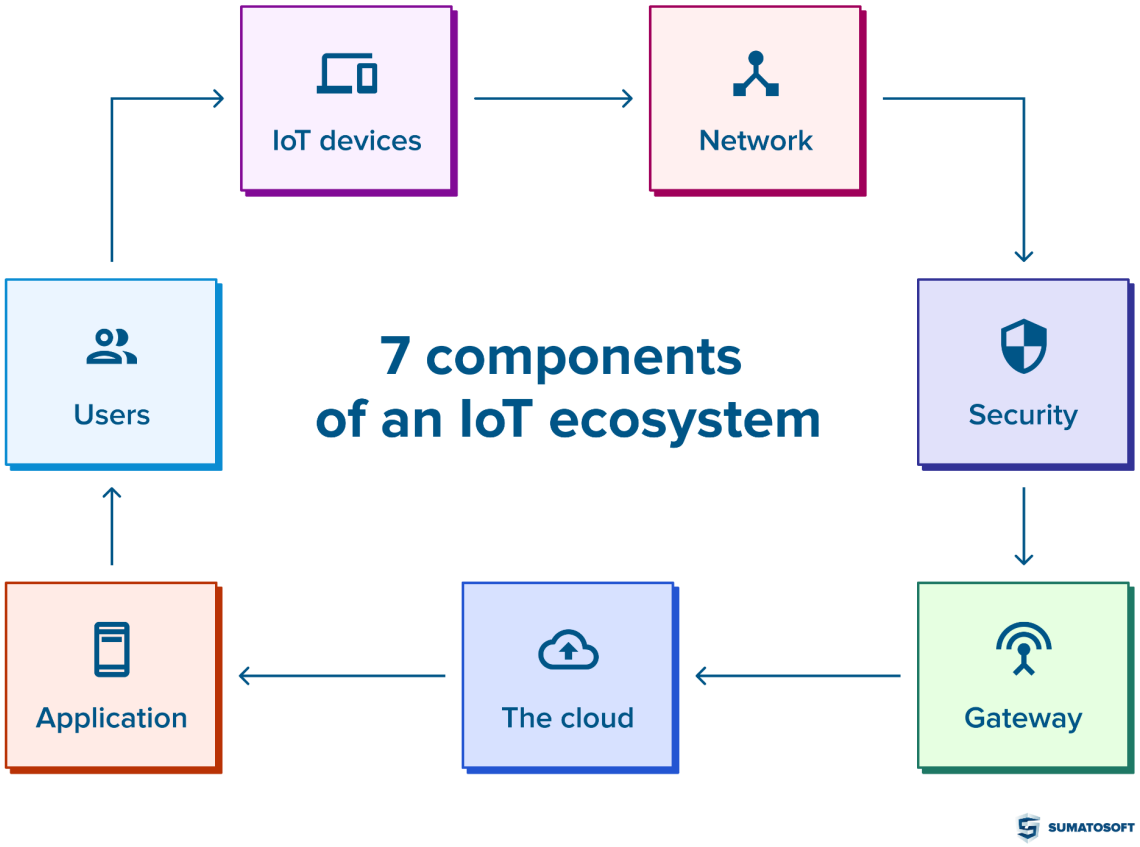
Since different groups of people build different IoT applications for their purposes, IoT software development creates numerous IoT ecosystems. These ecosystems can be a simple network with 20 connected devices like a smart home or a multi-level structure with a complicated and

broad network of devices that requires a sophisticated platform to manage all layers. Look at the video to understand to get the gist of an IoT system for personal use.

If we decompose the most complex IoT ecosystem with a middle layer into its building blocks, we get the next scheme: IoT devices gather the data and securely transfer it through the network to a gateway connected to the Internet that compresses the information and passes it to the cloud for further analyses to be later displayed in the application to provide users with meaningful insights.

Thus we listed 7 components of an IoT ecosystem:

- IoT devices
- security
- network
- gateway
- Cloud
- application
- users



7 components of IoT ecosystem

These components are sufficient to describe the most complex IoT ecosystem, although most ecosystems don't need them all.

The next step that is expected to be taken is to dive deep into the meanings of these components and describe them in detail. However, we have a better idea.

Component	Details
IoT devices	Physical devices that interact with the environment. There are two types of them: • Sensors – are devices that are supposed to gather information about the environment and measure its physical parameters like temperature, motion, people flow, etc. In other words, sensors convert physical phenomena into a digital form. • Actuators – are devices that perform a physical action on things after they get such a command. **An example:** actuators turn on the lights when sensors detect a movement within its operating radius. Important notes: as we have mentioned, the main benefit the Internet of Things provides is the data. That means that sensors must transfer the information (about detected movement in our case) to the cloud through the Internet. So when you enter the house and the lights turn on, you most likely don't become a participant of the Internet of Things ecosystem since the information about you entering the house is not transferred further to the cloud.
Network	The network is responsible for the communication within an IoT ecosystem between smart things, gateway, and the cloud. **An example:** a smart fitness bracelet tracks your heart rate and waits until you connect your smartphone with Bluetooth to transfer the data. After your smartphone gets your heart rate, it stores the data in some installed health app. The app then will sync with the cloud by transferring your heart rate through the Internet to cloud servers. The network makes sure that the data will not be corrupted during the transfer via Bluetooth and through the Internet.

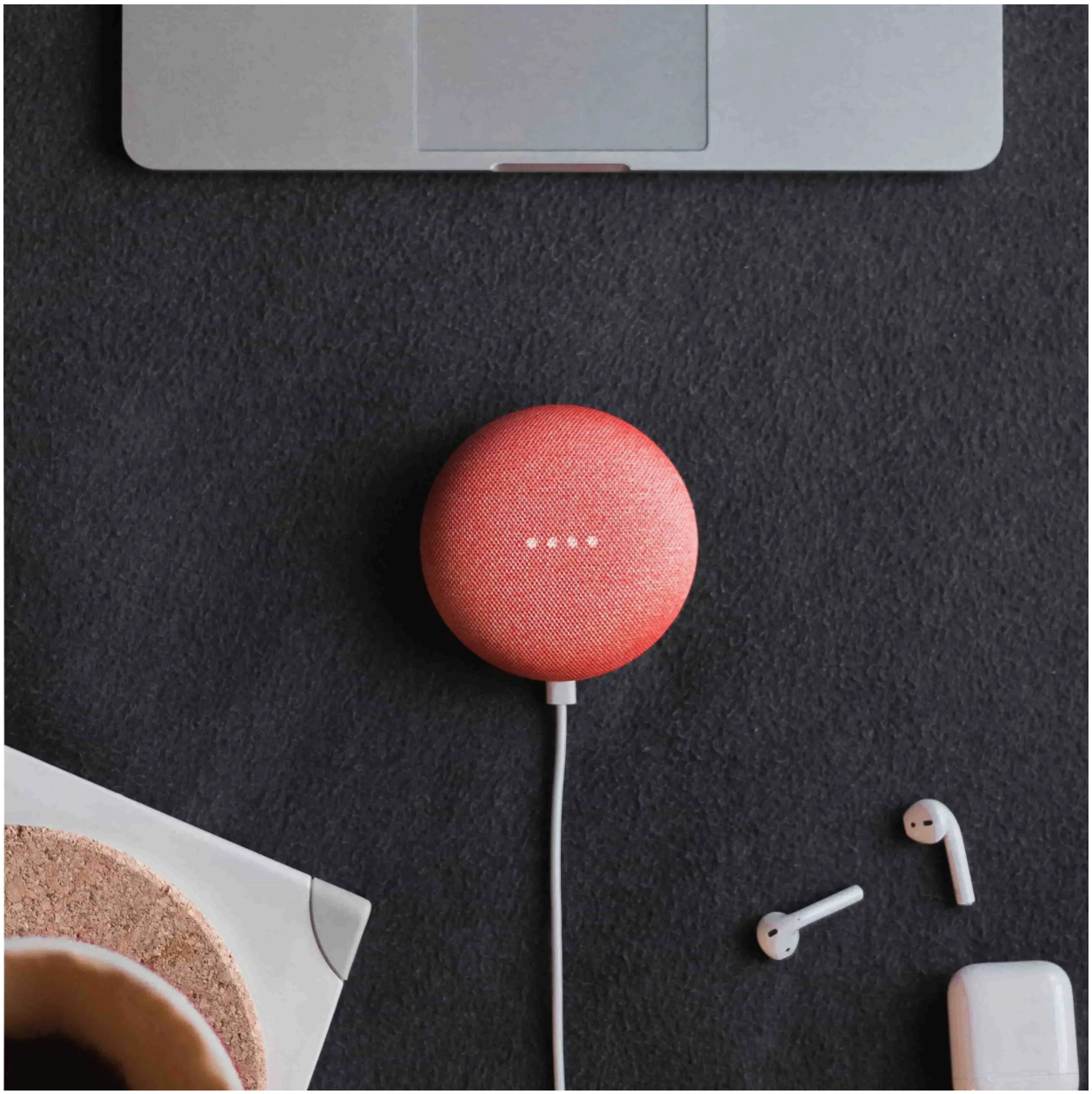
Component	Details
Security	The security component is responsible for access control to the IoT network, the security of data transfers, data leakage prevention, and scanning for malicious software. The security component is presented by firmware and software from security providers, such as Azure Sphere. **An example:** many IoT devices have non-existent or very simple passwords for authentication. That led to the emergence of botnets that are also known as “zombie armies”. An army is a group of hacked devices that are connected to the Internet and participate in DDoS attacks on websites.
Gateway	Gateway is a physical device that passes through itself data streams from sensors to the cloud and in the opposite direction. It also performs data preprocessing before the information will be transferred to the cloud. A gateway is not a necessary element since IoT devices can set connections to the Internet by themselves without a gateway as an intermediary. **An example:** You probably have a router at your home via which you connect to the Internet. You can consider the gateway as some sort of router (it even may look like a router as a fanless plastic box with buttons), but a bit complicated since it integrates data from thousands of devices, preprocesses it, and has some more responsibilities.

Component	Details
Cloud	The cloud is a cloud-based computer resource that is responsible for data storage, deep analysis, and management. In other words, it is a group of computers people get access to through the internet to use their compute capacity for some purpose. The cloud is enhanced by powerful analytic and visualization tools, Big Data algorithms, and Machine learning technology. **An example:** imagine you building the Internet of Things ecosystem with 10 000 connected devices that measure the physical parameters of the environment on your field crops. They collect the raw data and send it to your home computer to store it. The computer would get terabytes of information every day. Is its storage capacity enough? Probably not. Furthermore, the raw information is useless until you have an army of humans who can analyze it. Or you can use cloud technologies and get as much storage capacity as you need as well as get all the necessary tools to process and analyze the information. An example of the cloud in the Internet of Things is Cloud IOT core from google.
Application	Application is the graphical user interface that provides remote control and management devices connected to the Internet of Things ecosystem. **An example:** you left your smart home and you have doubts whether you locked the door. It's not a problem! Open the application on your phone and check. If the door is not locked, one click in the app is enough to lock the door.

Component	Details
Users	Users are all the people who affect the Internet of Things ecosystem and use it for their purposes. Users comprise people with personal IoT gadgets, researchers who use analytics from the IoT cloud, staff who use the Internet of Things in their operational processes, stakeholders who reap the benefits from huge industrial IoT solutions. IoT ecosystems are supposed to serve people's needs, boost efficiency, improve the standards of living, and quality of life. Users are those who declare business goals and vital postulates that will become the basis for the Internet of Things ecosystem. **Example:** You are with a high probability. If there is a fitness bracelet/smartwatch on your wrist, you are a user in the IoT ecosystem.

7 Components of an IoT Ecosystem – Detailed

Before we start, it's worth mentioning that there is no single, officially recognized structure of the Internet of Things ecosystem. Some components are mandatory like IoT devices, some are optional like gateways. The more components the ecosystem includes the more focus it has on finer aspects of the Internet of Things.



#1 Component: IoT Devices

IoT devices are the layer of sensors, actuators, and smart objects that gather information about the environment and measure physical parameters.

As we have already mentioned, the basic elements of the Internet of Things ecosystem are sensors and actuators (or just “things”). Sensors are the perception of the IoT system whose main function is to get information from the environment and transform it into data.

It’s a rare case when the Internet of Things ecosystem features only one type of sensor or actuator. There are numerous types of sensors and every type has its sub-categories of sensors. We want to mention two of the most common sensors and two of the most essential for improving the ecological state on Earth:

- **Temperature sensor** – one of the most common and popular. Different industries benefit from these sensors since they can measure the temperature of an industrial machine to check its health, constantly track the temperature of a sick human, or monitor the soil conditions for farmers. Sub-categories: thermocouples, resistor temperature detectors, infrared sensors, etc.
- **Proximity sensors** – a well-known type of device since there are thousands of homes with such types of sensors to save energy on lighting when no one is around. Sub-categories: inductive sensors, photoelectric sensors, ultrasonic sensors.
- **Water quality sensor** – especially important due to the pollution of the oceans. These sensors can help to monitor the condition of water and detect sources of pollution in real-time. Sub-categories: chlorine residual sensor, turbidity sensor, pH sensor.
- **Chemical sensors** – they monitor the chemical changes in the air, which is extremely important in big cities where the issues of air pollution continue to worsen. These sensors are also helpful in industrial environmental monitoring, harmful chemical detection, and radioactive detection. Sub-categories: chemical field-effect transistor, hydrogen sulfide sensor, potentiometric sensor.

#2 Component: Security

Security – it is the component that encompasses all other components, provides security of data transfer, and prevents unauthorized connections outside the Internet of Things ecosystem. In recent years the number of IoT-based DDoS attacks grew dramatically. That is why any IoT system needs a strong security level that protects at least from the most common vulnerabilities. The security level has a wide array of responsibilities, like:

- **Access control to IoT network.** IoT devices may trust the local network to such a level that no further authentication is required. Anyone who connects to the network gains access to all devices within it, making broken authentication issues especially acute.
- **Preventing data breaches** while transferring data across the network. The data must be encrypted across the IoT system with protocols, like AES, DES, DSA, and others.
- **Scanning for malicious software.** In some cases, software bugs can result in the attackers running their own code on the IoT device. It's necessary to patch software versions when any vulnerability is detected.

There are various firmware and embedded security providers to secure the Internet of Things ecosystem, such as Azure Sphere, LynxOS, Mocana, Spartan, Forescout, Symantec, etc.

Unfortunately, most Internet of Things providers and IoT device manufacturers overlook even the **basic security guidelines**. They are:

- The device boot process must be secured from running inappropriate code pieces
- Cryptographic keys must be used to run any command on the devices. It's especially important in IoT update management.
- All control commands and information should go through a gateway to avoid direct access to the device outside the network.
- Whenever a new security breach is detected all IoT devices should install security patches from it.

#3 Component: Network

The network is the core logistics part of the Internet of Things ecosystem. The network is also called a connectivity layer. It is responsible for all communication within the IoT system: the interconnection of smart things, transferring data and commands between IoT stages, and connection to the cloud.

There are two ways of communication:

The first way of **communication takes place locally within a Local Area Network (LAN)** between IoT devices and smart gateways through short-range wireless communication protocols. This way of communication is optional because sensors can connect to the cloud directly through the Internet using TCP/IP protocol. However, the connection through non-IP protocols consumes less power since devices connect to local smart gateways instead of trying to access the main server in the cloud.

The most popular short-range protocols for the Internet of Things architecture are as follows:

- WiFi
- Bluetooth and Bluetooth Low Energy (or Bluetooth LE for lower-powered devices that generate less data)
- ZigBee – a universal solutions interlacing all smart devices
- Near Field Communication (NFC)
- Radio Frequency Identification (RFID)
- Sigfox

- LoRaWAN

If the system needs to cover long distances in the range of kilometers, it can use Low Power Wide Area Network (or LPWAN) that is designed for wireless data transmission across long distances.

The second way of communication occurs when **the data is transferred from things to the cloud** in cases where there is no smart gateway or in the case of communication between smart gateways and the cloud. The network layer establishes a link between the Local Area Network and the Internet. The basic protocol here is the IPv6 protocol.

#4 Component: Gateway

IoT gateway is a physical device or virtual platform that serves as an intermediary between IoT devices and the cloud.

There are several **main functions of the IoT gateways**:

- control the data flow in the Internet of Things ecosystem. The data flow goes through the gateway from devices to the cloud and in the opposite direction.
- ensure the safety of the transfer of the information in both directions.
- pass commands from the cloud to IoT devices.
- preprocess the data before sending it to the cloud. Gateways filter, aggregate, summarise, and cluster traffic from different devices.
- save the power of the IoT devices since communication through the internet consumes a lot of power, while low energy technologies like Bluetooth low energy don't.
- reduce latency of responses to IoT devices. Some devices need a real-time response from the system. Communication with the cloud can take a while, while gateways can be programmed to handle some typical issues and provide instant responses to devices.

#5 Component: Cloud

The cloud is a cloud-based computer resource responsible for data storage, deep analysis, and management. In other words, it is a group of computers people get access to through the internet to use their compute capacity for some purpose.

The cloud is the place where a big pile of raw data from sensors is transformed into neat small piles of valuable information. The most popular vendors of cloud computing are Microsoft Azure and AWS IoT. The cloud can be powered with analytics software, visualization tools, AI, and machine learning for in-depth analysis and processing of the data.

One of the main advantages of the cloud solution is that they are easily scalable which is a vital requirement for building an effective IoT system.

#6 Component: Application

When software development companies build software for the whole Internet of Things ecosystem they deal with all 7 components and build a system that covers the requirements on all levels. However, IoT application is the tip of the iceberg in IoT software development. An application is a place where users can interact with the Internet of Things ecosystem. The interaction becomes possible thanks to the graphical user interface where users can look through analytics and reports, control the system, and manage devices.

The list of technologies used in the development includes:

Programming languages: C/C++, Python, Ruby, JavaScript

Development frameworks: Node.Js (Node-Red for rapid prototyping), Ot, IoT.js, Device.js, Eclipse IoT (Kura, SmartHome), AngularJS

3d-party APIs: Google Assistant, Google Home (Actions on Google), Google Vision, Apple HomeKit, MI Light, Cortana, Alexa Voice Service, Philips Hue, Android Things

#7 Component: Users

Users are perhaps the most essential component among all 7 components of the Internet of Things ecosystem. Users have two roles:

- They use an IoT ecosystem for their purposes. The opportunities the Internet of Things ecosystem brings become a basis for valuable insights for all types of users. IoT has a great impact on businesses and the world economy, it changes the existing business models and leads to the emergence of new ones. IoT sensors and applications can become professional health assistants that measure biometric data of the patient and help to make a more accurate diagnosis. The Internet of Things transforms all 6 stages in the supply chain management while businesses experience growth thanks to machine downtime reduction and automatization. The impact of the Internet of Things ecosystem is enormous.
- Users define what the IoT ecosystem will do. The Internet of Things ecosystem is supposed to serve people, satisfy their needs, and provide particular information which helps to achieve users' goals. The IoT ecosystem is built by people, for people, and with a focus on people's needs.

Who can be users:

- People who use IoT gadgets for personal use
- Researchers
- Staff (doctors, warehouse workers, carriers, engineers, etc.)
- Stakeholders and top managers

That is all you need to know about the 7 components of an IoT ecosystem. If you would like to learn more or build the Internet of Things ecosystem for your business, feel free to contact a Sumatosoft team.

SumatoSoft is a software development company that follows the principle of transparent cooperation and excellence of work. We're a team of skilled and creative people who specialize in the development of top-quality software for our clients.

SUMATOSOFT

Thank you for reading!

Any questions? Drop us a line!

Headquarters

One Boston Place, Suite 2602
Boston, MA 02108, United States

Other ways to get in touch

info@sumatosoft.com
sumatosoft.com