

Big-data practical example – The Internet of Things

In addition to smartphones, many other devices also collect and autonomously exchange data. They communicate with each other, for example, via a wireless network, and can be controlled remotely. These developments are used, for example, in modern manufacturing facilities. Collectively, they are referred to as the Internet of Things. This technology is intended to make people's everyday lives easier. In the process, the devices collect a wide variety of data, including users' personal information.

The following text explains what devices are involved, how they collect data, and what happens with these data.

What is the Internet of Things?

In the Internet of Things, devices and objects such as mobile fitness trackers, navigation devices, and smartwatches are connected with the Internet. In homes, interactive speakers or networked thermostats, lighting fixtures, blinds, and household appliances are used. Living quarters with numerous networked applications are called a "smart home".

Other objects acquire information such as the user's location, movement data, or pulse rate via built-in sensors, and yet others serve as a control center for household appliances. Most of these objects can be read and operated remotely. They have their own "identity" through which they can be recognized, for example, an Internet Protocol (IP) address, a device ID, or information stored on a built-in chip that transmits data via radio-frequency identification (RFID) technology. In technical terms, this means that they are recognizable and unique.

The Internet of Things also includes objects such as biometric earbuds and electronic tattoos, which use built-in sensors to measure body temperature or muscle tension and skin moisture. It also includes "wearables", socks, T-shirts and underwear with corresponding sensors that, for example, measure the number of steps taken or heartbeat.

The devices and objects transmit the collected measured data either to a smartphone app often via Bluetooth or to a service provider specialized in such data directly via a wireless network.

The versatile smartphone

Smartphones play a key role in the Internet of Things.

First, they themselves have sensors including those for acquiring coordinates (GPS, which is used with fitness trackers) and other movement data that are measured during athletic activities such as through acceleration sensors or that are important for navigation systems. Other components measure air pressure (barometer), the ambient temperature (thermometer), or humidity (hygrometer) – typical meteorological data that prove useful for evaluating weather developments, for example, during travel or nature outings.

Second, smartphones are equipped with short-range radio technologies such as wireless networks, Bluetooth, and NFC chips. NFC is the abbreviation for near-field communication, a radio technology that reaches only a few centimeters and is used for contactless payment of small amounts at supermarkets or department stores, for example. With these connection technologies, smartphones can receive the uninterrupted flow of data from the mentioned devices – and control the devices interactively.

Third, smartphone apps can presort and process the received data, and sometimes even analyze the data intelligently.

What does this have to do with big data?

Even with single users, immense volumes of data accumulate on a daily and weekly basis due to the numerous devices of the Internet of Things. These volumes are also necessary to be able to identify how someone behaves over a longer period and to draw conclusions. Thousands or even millions of users ensure regular masses of data. Typical big-data applications process these data to help users improve their own physical fitness, to track the development of household energy consumption, and to carry out other statistical analyses.

What is worrying about this?

Many manufacturers of Internet of Things devices state that they use big-data analyses primarily to improve their products and services, for instance, to determine whether particular functions are seldom used or others are frequently demanded. However, it is known that some manufacturers share the collected and processed usage data with other providers. These providers subsequently develop personalized advertising from the usage data, for example. In this respect, the Internet of Things deserves particular attention since the devices frequently record very comprehensive and personal data, for example, from the user's own home or related to the user's health. At the same time, it is frequently unclear when devices that have cameras or microphones are actually recording and when they are not. These devices thus enable extensive surveillance of individuals.