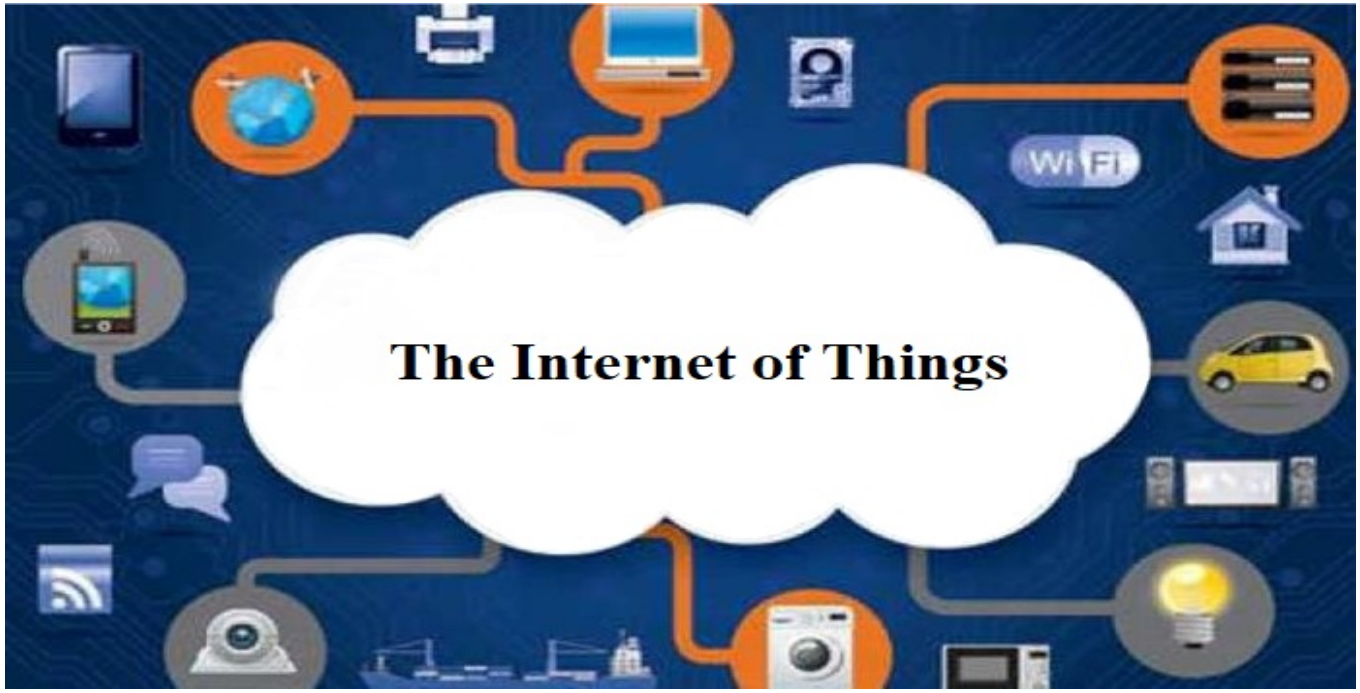
The Internet of Things (IoT).

The Internet of Things (IoT) is a concept of a computing network of physical objects ("things") equipped with built-in technologies for interaction with each other or with the external environment, which considers the organization of such networks as a phenomenon capable of reshaping economic and social processes that eliminates the need for human participation from part of the actions and operations.

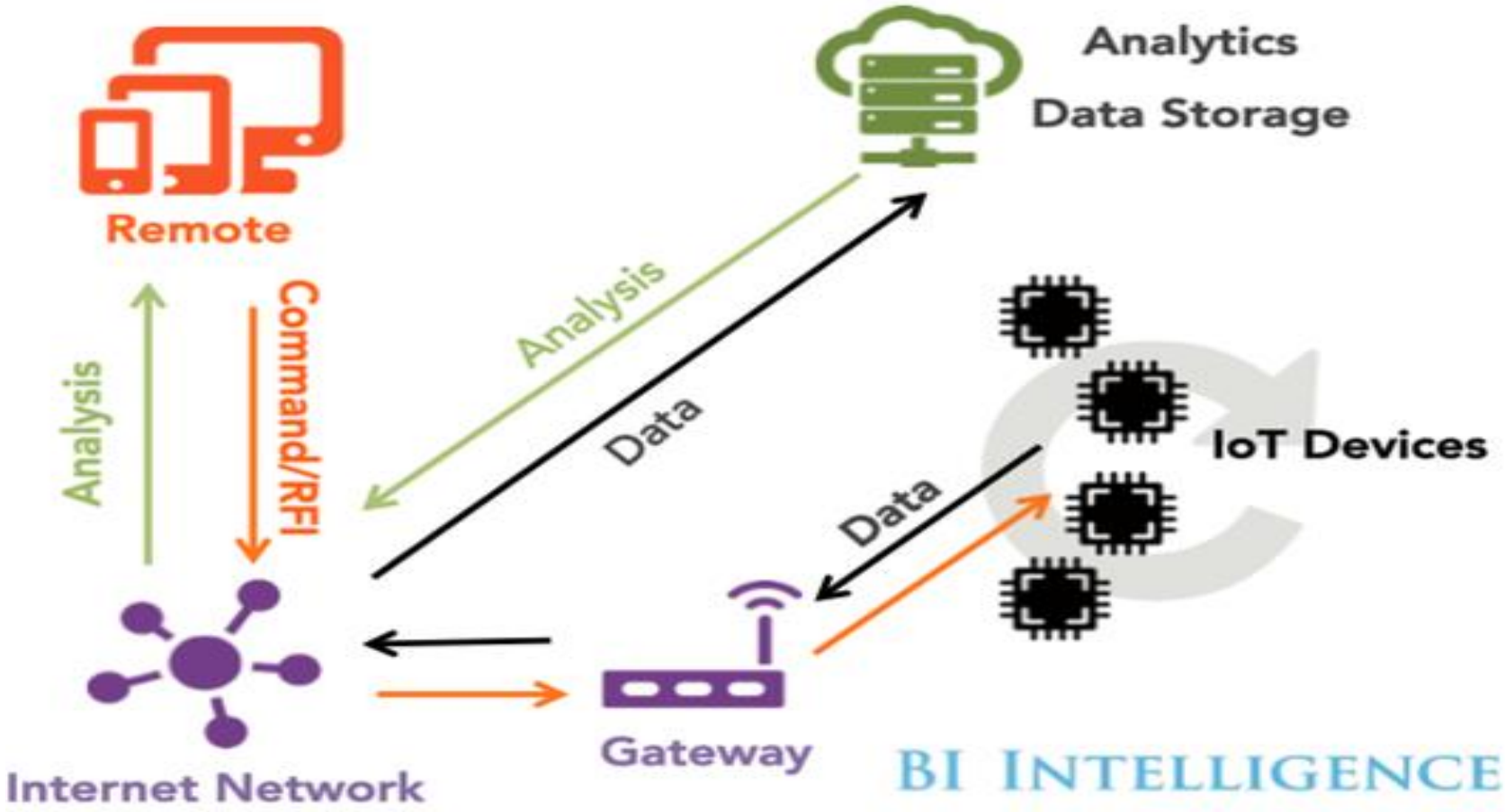
The term "Internet of Things" appeared in 1997. Since then, the Internet of Things has completed the transition from simple radio frequency tags to an ecosystem and an industry. Until 2012, the idea of connecting things to the Internet mostly referred to smartphones, tablets, PCs, and laptops. Before 2000, most devices that could be connected to the Internet were computers of various sizes.

Filling the concept of "internet of things" with various technological content and implementing practical solutions for its implementation since the 2010s is considered a stable trend in information technologies, first of all, thanks to the widespread spread of wireless networks, the emergence of cloud computing, the development of machine-to-machine interaction technologies (Machine to machine (M2M)), the beginning of an active transition to IPv6 and the development of software-configurable networks.

The concept assumes that the Internet of Things is able to seriously affect the development of modern society, as it will allow many processes to take place without human intervention.



The Internet of Things Ecosystem



The Industrial Internet of Things is one of the largest segments of the Internet of Things in terms of the number of connected devices and the degree of usefulness of these services for the production and automation of enterprises. This segment traditionally serves as an operational and technological base. This includes hardware and software monitoring of physical devices.

Examples of industrial Internet of Things applications:

- **Preventive maintenance of industrial equipment;**
- **Productivity growth thanks to real-time demand;**
- **Energy saving;**
- **Safety systems, such as temperature measurement, pressure measurement and gas leak control;**
- **Expert system for the production shop.**
- **Sensors (intelligent sensors/executive mechanisms): embedded systems, real-time OS, uninterruptible power sources;**

- **• Communication systems with sensors: the coverage area of wireless personal networks is up to 100 m. Low-speed, low-power information channels are used for data exchange between sensors;**
- **• Local computer networks (LAN);**
- **• Routers, edge devices (Edge Device);**
- **• Global computing network: cellular operators, satellite operators, operators of low-power global networks.**
- **• Cloud: infrastructure as a service provider, platform as a service provider, database developers, streaming and batch data processing service providers, data analysis tools, software as a service provider, machine learning services;**
- **• Security: when all elements of the architecture are brought together, issues of cyber security arise. Security applies to every component: from sensors of physical quantities to CPUs and digital hardware, radio communication systems and data transmission protocols. Security, reliability and integrity must be ensured at every level. There should be no weak links in this chain, as the Internet of Things will become the main target for hacker attacks in the world**.

General principles of construction and architecture of IoT.

For practical implementation, all surrounding objects and devices must be equipped with miniature identification and sensor (sensitive) devices. Then, with the necessary communication channels, it is possible not only to track these objects and their parameters in space and time, but also to manage them, as well as to introduce information about them into the general "smart planet".

In general, from the information and communication point of view, the Internet of Things can be written in the form of a symbolic formula:

$$IoT = Sensors + Data + Networks + Services$$

Architecture of the Internet of Things.

The connection of "smart things" (Smart Things) into a single network provides critically important qualitative changes for the development of human life.

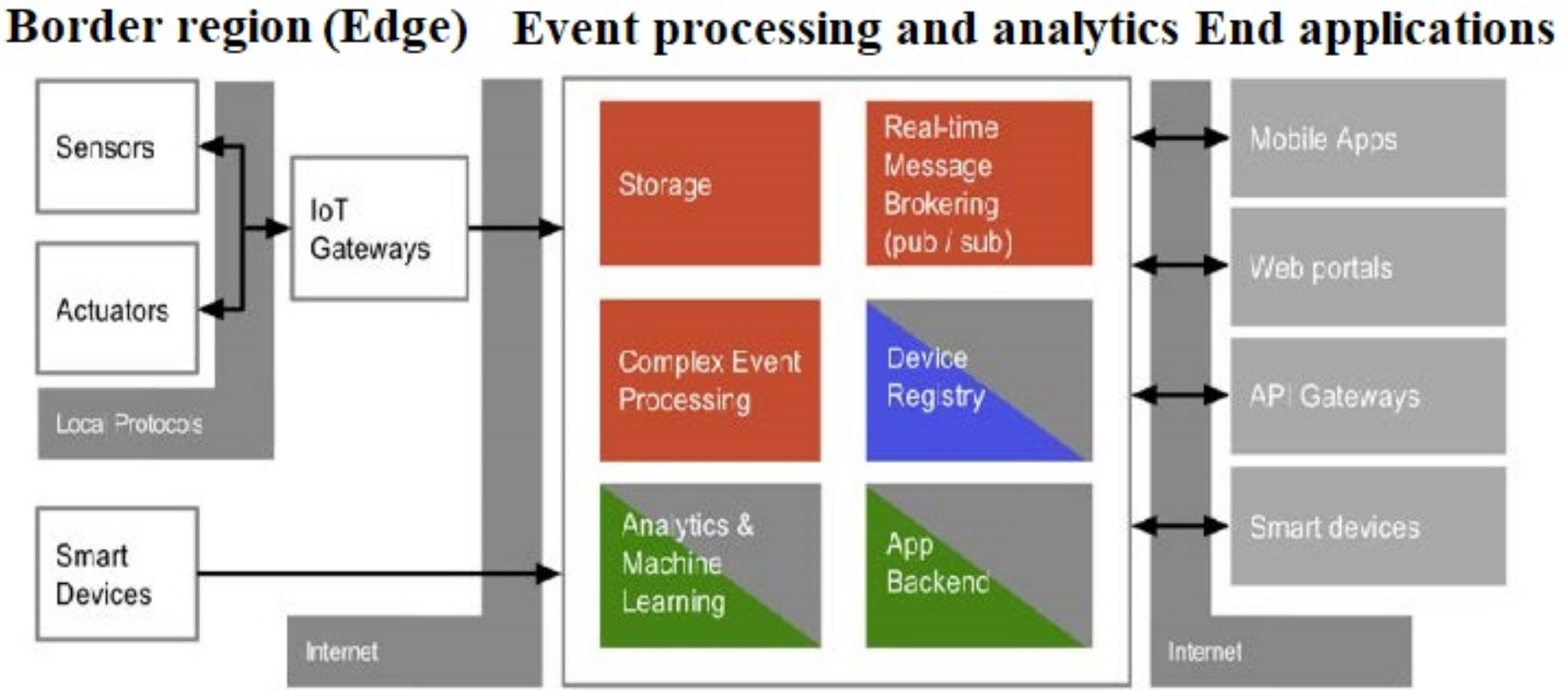
The connection of smart objects into a single network using the IP protocol forms a network of networks, producing a large amount of a wide variety of telemetry data. And the value of the received information is completely determined by application-level protocols operating on top of the network.

The main task is the identification of each element. Given the required bit rate, an IPv6 address allocated to each device in modern networks is best suited for this.

Smart objects, which have a unique identifier depending on the design, are able not only to transmit data streams collected by sensors, but also to transmit commands to change the state of devices connected to them.

Measures to ensure security can be conventionally divided into the following areas - connection, identification, traffic encryption and application security.

The architecture of the Internet of Things differs depending on the implementation. One example of the architecture is shown in the figure below.



Sensors and power.

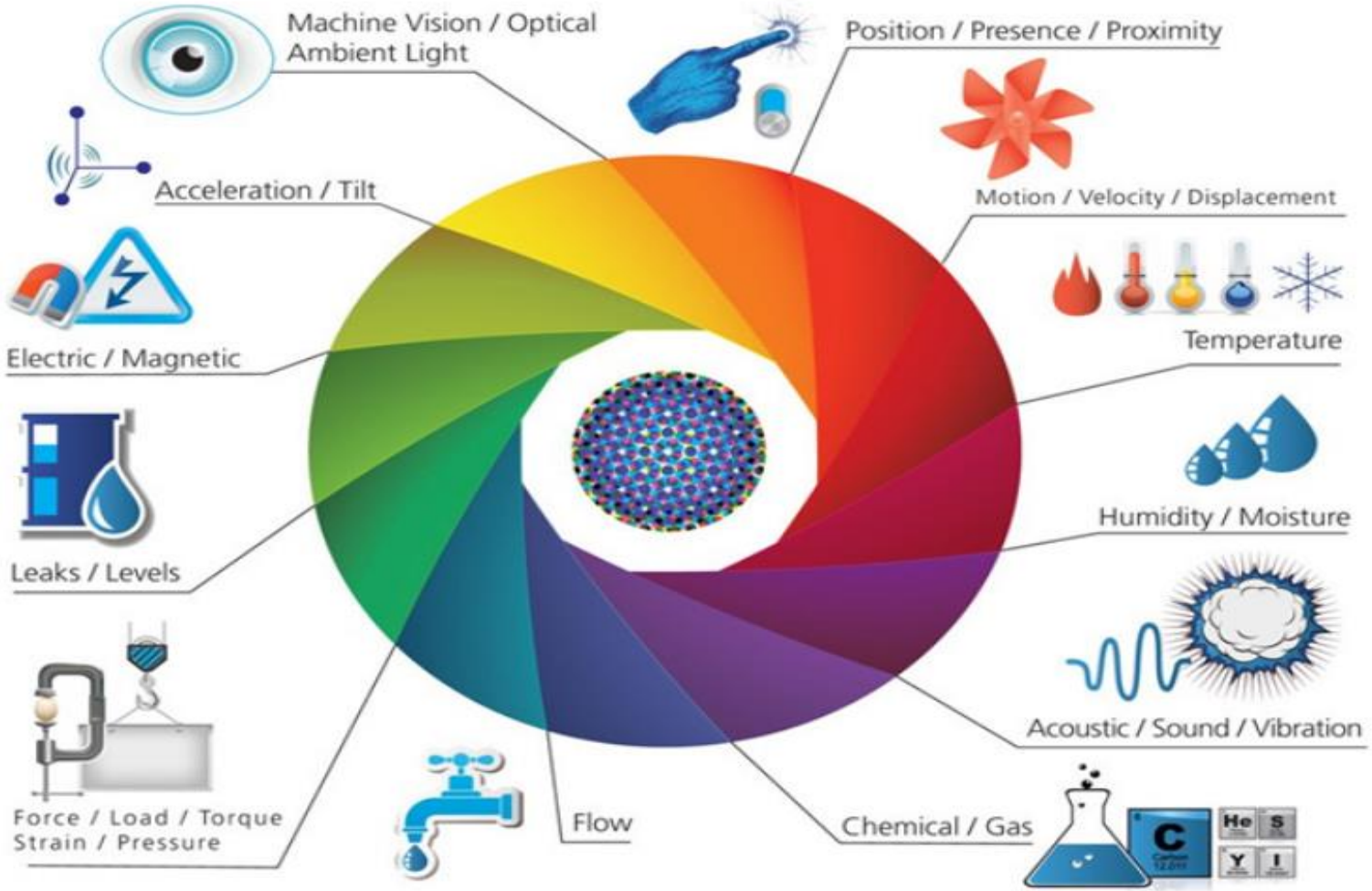
The Internet of Things is mostly related to a physical action or event. It forms a reaction to some factor of the real world. Sometimes, a single sensor can generate a huge amount of data, for example, an acoustic sensor for a preventive inspection of equipment. In other cases, just one bit of data is enough to convey vital information about the patient's health.

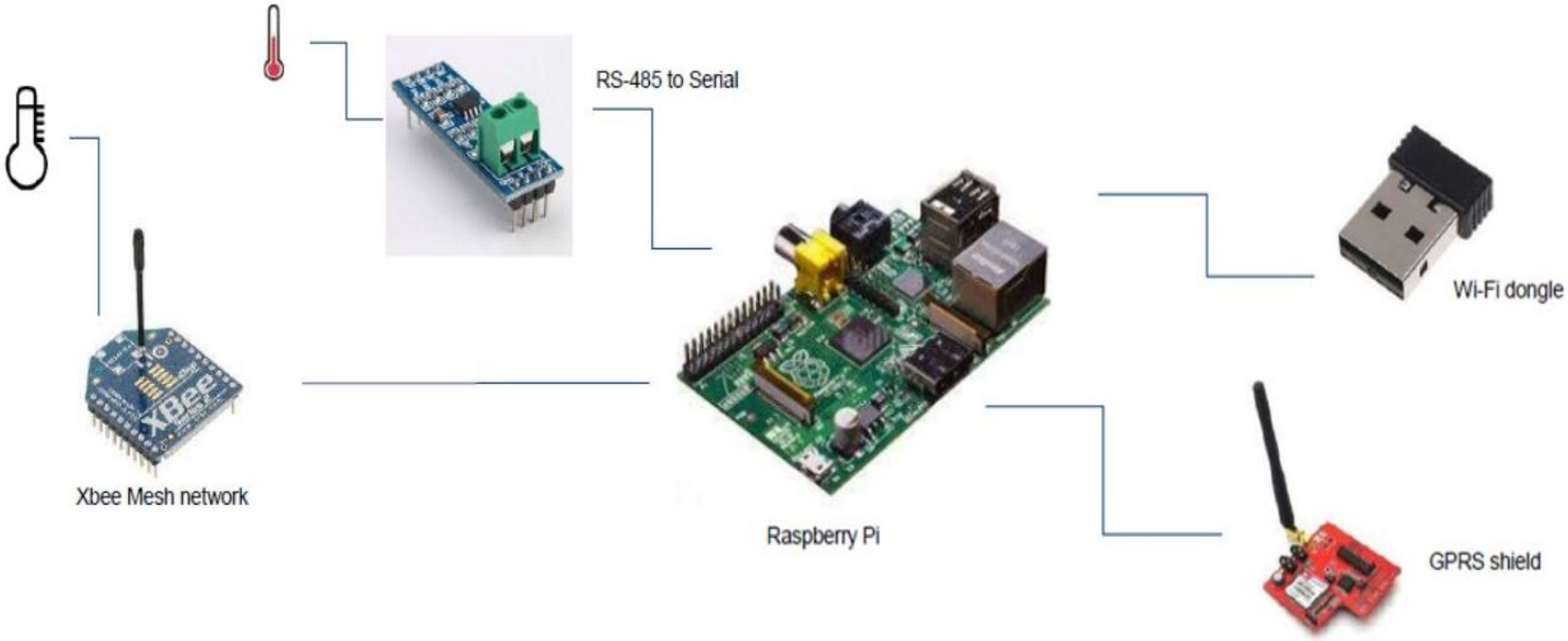
Data transfer.

A lot of attention during the development of IoT is paid to the establishment of connections and the operation of networks.

The Internet of Things would not exist without reliable data transfer technologies from the most remote and unfavorable areas to the largest data collection centers of Google, Amazon, Microsoft and IBM.

The phrase "Internet of Things" contains the word "Internet", so it is necessary to study issues related to network technologies, data exchange and even signal theory. The basic support of the Internet of Things is not sensors or programs, but the ability to establish a connection.


Machine Vision / Optical
Ambient Light
Position / Presence / Proximity
Acceleration / Tilt
Motion / Velocity / Displacement
Electric / Magnetic
Temperature
Leaks / Levels
Humidity / Moisture
Acoustic / Sound / Vibration
Force / Load / Torque
Strain / Pressure
Flow
Chemical / Gas

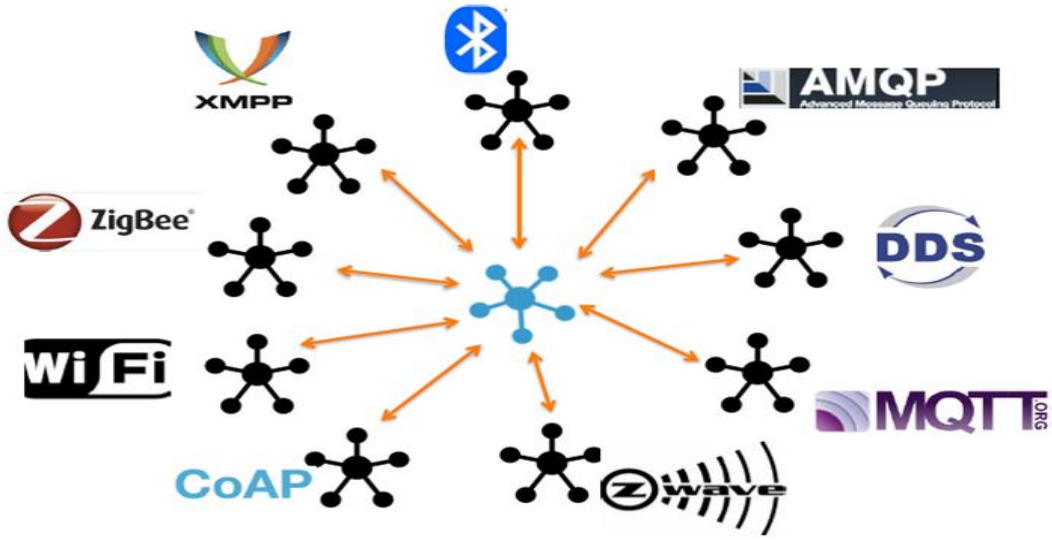

RS-485 to Serial
Wi-Fi dongle
Xbee Mesh network
Raspberry Pi
GPRS shield

Routing.

To transfer data from sensors to the Internet space, two technologies are needed: a router-gateway and basic Internet protocols that ensure the efficiency of data exchange.

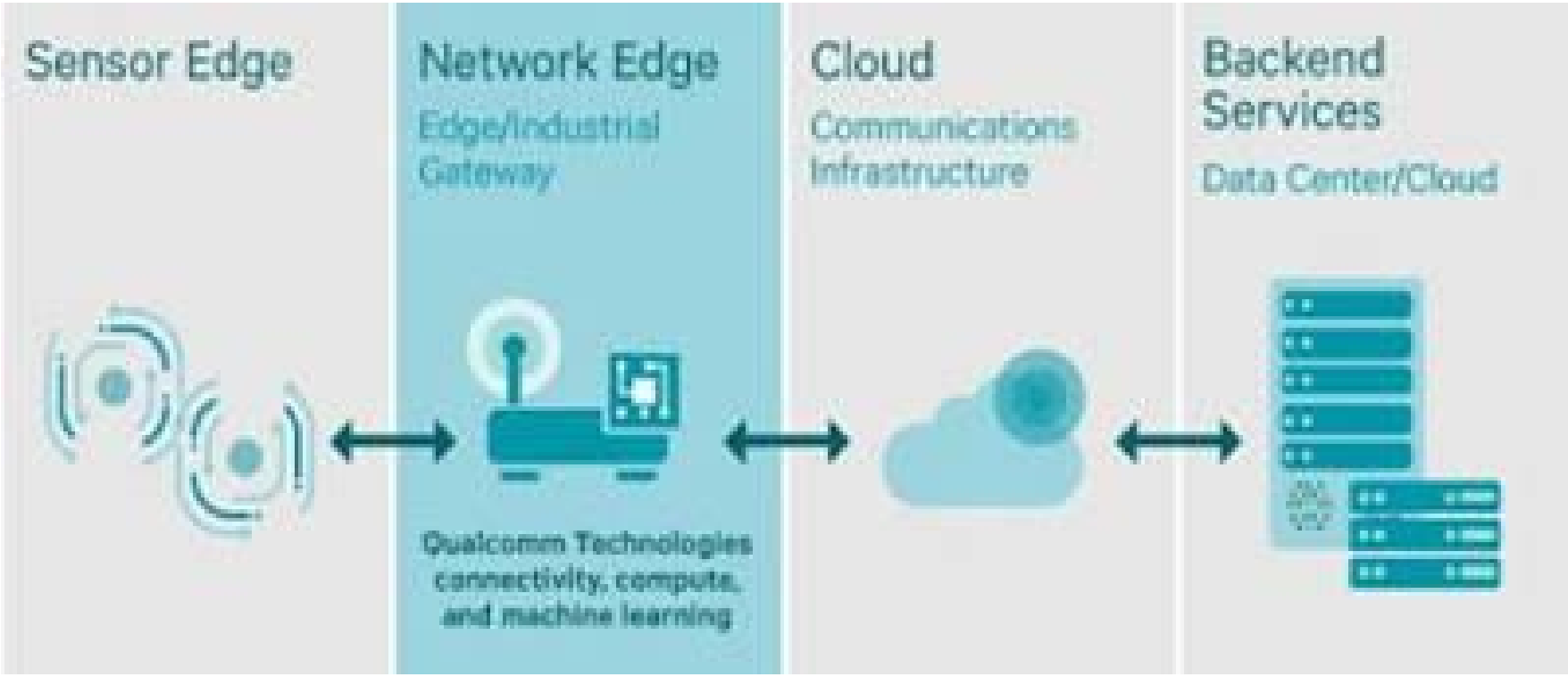
A router is particularly important in aspects such as security, management, and data routing.

The router plays an important role in creating virtual private networks, virtual local networks and software-defined wide area networks. They can literally contain thousands of nodes served by a single edge router, and to some extent the router serves as an extension to the cloud (edge device).



Fuzzy and boundary computing, analytics and machine learning.

Data that was obtained by converting an analog physical effect into a digital signal can have a lot of weight. This is where analytics tools and rule processors of the IoT system come into play. The degree of complexity of implementing an IoT system depends on what solution is being designed.



Characteristics of the Internet of Things:

• Interconnection - all devices interact through a global or local infrastructure of information exchange.

• Device-oriented services - the Internet of Things is able to ensure semantic consistency between physical objects of the real world and their information presentation in virtual space and unite physical devices taking into account rules and restrictions.

• Heterogeneity - devices in IoT are heterogeneous by definition and can belong to different networks and hardware platforms, which is not an obstacle to interaction.

• Dynamics - the state of devices changes constantly: on and off, contextual and technological information, including location and speed. The number of connected devices can also change dynamically.

• Scalability - the number of devices that will "communicate" and receive a controlling influence will exceed ten times the number of nodes in the current Internet network. It is clear that the number of communications that can be initiated by devices will radically exceed the possible number of human-initiated connections. Therefore, the questions of data interpretation come to the fore, with the aim of their further application.

Levels of the Internet of Things.

The Internet of Things includes three levels:

- **Components;**
- **Structural blocks;**
- **System of systems.**

Components are designed specifically for a specific application, which means - for solving specific problems.

Structural blocks are elements common to many solutions, extremely important for successful operation.

The system of systems describes unique ways of possible unification and integration of structural blocks, as well as their deployment in various industries.

Classification of IoT systems.

By application: household - industrial.

Industrial can be divided according to the scope of application: transport, agriculture, medicine, military, etc.

According to the importance of the consequences of use: ordinary - critical.

According to movement capabilities: static - dynamic.

According to the requirements for signal transit time:

Real time - little critical to time.

By degree of protection:

Strongly protected - weakly protected

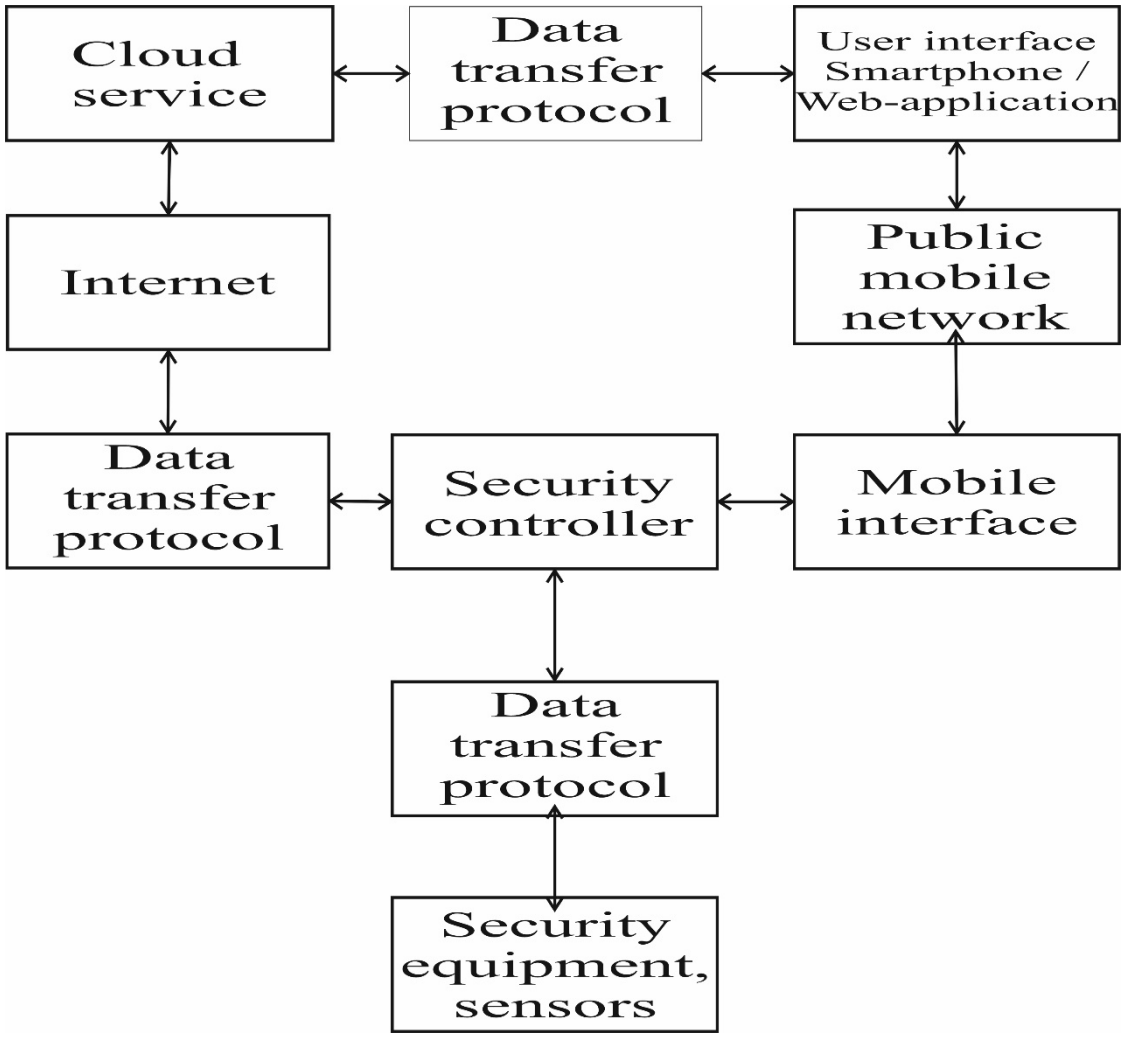
There are factors capable of slowing down the development of the Internet of Things. Of them, three are considered the most serious: the transition to the IPv6 protocol, the power supply of sensors, and the adoption of common standards.

So far, the implementation of the Internet of Things does not take place on a global scale, but within companies. The technology of smart things is able to increase labor productivity, first of all, in the production segment, logistics business, transport and energy companies.

The difficulty of implementation lies in the fact that no manufacturer has a complete solution that includes all components.

Development of a home security system based on Internet of Things technologies.

A cost-effective IoT-based smart home security system platform that provides cloud data for applications is proposed. The smart security system includes a sensing network of home condition monitoring devices via wireless communication in the ISM range, a home security system control controller with a connection to the Internet using a wireless Wifi connection, and a backup way of notifying the user is realized by an SMS message via the GSM cellular network. cloud server and application for mobile phones on the Android operating system. The developed application combines the use of a cloud server, client sensors and a database. The hardware and software implementation of IoT-based home security system and their relative functions are also clarified.



Structural diagram of the smart home security system.

The structure of the security system is conditionally divided into three parts:
- Microcontroller unit,
- Web server,
- User interface.

The microcontroller part consists of:
- Sensors and security equipment responsible for round-the-clock monitoring Surveillance room if the system is on. Provides detection of unwanted movement of people in the house.
- Data transfer protocol (DTP) - is an interface of interaction between sensor units and the controller.
- The security controller is responsible for the analysis of data received from the sensors, the transfer of information about the status, direct notification of the system about interference with private property in case of data deviation from the norm.

The web server part consists of:
- Database stores details of all home devices and their current status. User data and their authentication keys.
- Data transfer protocols - a set of logical level interface agreements that define data exchange over the Internet between the web server and microcontroller parts.

User interface.

A user (subscriber) who gets access to his home in a private manner can request information about the state of the device from the database and change it

The role of the user interface in our system is played by an application for mobile smartphones.