MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL AVIATION UNIVERSITY
FACULTY OF AERONAVIGATIONS, ELECTRONICS AND TELECOMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATION AND RADIO ENGINEERING SYSTEMS

ADMIT TO DEFENCE
Head of the Department

_____ R. Odarchenko
"_____"_____2022

DIPLOMA WORK
(EXPLANATORY NOTE)

BACHELOR'S DEGREE GRADUATE
BY SPECIALITY "TELECOMMUNICATIONS AND RADIO ENGINEERING"

Topic: « Fog computing for IoT infrastructure improving »

Performer: _____ M. Suzdaltsev
(signature)

Supervisor: _____ I. Terentieva
(signature)

N-controller: _____ D. Bakhtiyarov
(signature)

Kyiv 2022

NATIONAL AVIATION UNIVERSITY

Faculty of aeronavigations, electronics and telecommunications
Department of telecommunication and radio engineering systems
Speciality: 172 "Telecommunications and radio engineering"
Educational professional program: Telecommunication systems and networks

ADMIT TO DEFENCE
Head of the Department

R. Odarchenko
"_____"_____2022

TASK
for execution of bachelor diploma work

Maksym Suzdaltsev
(full name)

1.Topic of diploma work: «Fog computing for IoT infrastructure improving » approved by the order of the rector from «25» April 2022 №433/ст.

2. The term of the work: from 25 April 2022 to 10 June 2022.

3.Initial work data: Frequency of processor: 1 GHz; 1.5 GHz. Memory: 512 Mb RAM; 2 GB, 4 GB or 8 GB SDRAM. Wireless: 802.11 b/g/n wireless, LAN Bluetooth 4.1, Bluetooth Low Energy (BLE). 2.4 GHz and 5.0 GHz IEEE 802.11ac wireless, Bluetooth 5.0, BLE.

4. Explanatory note content: Introduction. Introduction to the concept and general provisions of the Internet of Things and Cloud Computing. The main concepts of Fog Computing and it is implementation in Internet of Things. Development and analysis of the platform with the application of the Internet of Things on the basis of Fog Computing with the use of Cloud-Native technology and LoRaWAN protocol.

5. List of required illustrative material: figures, tables, algorithms.

6. Work schedule

№ n/p	Task	Term implementation	Performance note
1.	Develop a detailed content of the sections of the thesis graduated work	25.04.2022-30.04.2022	Done
2.	Introduction	01.05.2022-06.05.2022	Done
3.	Introduction to the concept and general provisions of the Internet of Things and Cloud Computing	07.05.2022-16.05.2022	Done
4.	The main concepts of Fog Computing and it is implementation in Internet of Things	17.05.2022-23.05.2022	Done
5.	IoT network architectures based on LoRaWAN protocol	24.05.2022-05.06.2022	Done
6.	Elimination of shortcomings	03.06.2022-10.06.2022	Done
7.	Preparing the electronic report and illustrations	11.06.2022-12.06.2022	Done

7. Date of issue of the assignment: “25” April 2022.

Supervisor _____ I. Terentieva
(signature) (full name)

Accepted task for execution _____ M. Suzdaltsev
(signature) (full name)

ABSTRACT

Graduate work on the topic «Information and communication system for Online banking». It contains 85 p., 9 tables., 18 figures., 48 references.

KEYWORDS: CLOUD COMPUTING, EDGE COMPUTING, FOG COMPUTING, INTERNET OF THINGS.

The object of study is the Internet of Things and its architectures, protocols and characteristics.

The subject of research is the Fog Computing and its connection with other types of Computing's and Internet of Things.

The purpose of the thesis is to analysis of the architecture, model, and principle of operation of the Internet of Things. Carrying out a comparative analysis of the characteristics of protocols and data transmission technologies. Consideration of Fog Computing, their comparative characterization with Cloud and Boundary Computing, and analysis of the implementation of the Internet of Things.

Research of methods – an elementary platform of Internet of Things based on Cloud-Native technology and 3 network architectures based on the LoRaWAN protocol. Raspberry Pi Zero with 1 GHz, single-core CPU, 512 Mb RAM of memory; wireless support of 802.11 b/g/n wireless, LAN Bluetooth 4.1, Bluetooth Low Energy (BLE) and Raspberry Pi 4 Broadcom BCM2711, Quad core Cortex-A72 (ARM v8) 64-bit SoC @ 1.5 GHz; 2 GB, 4 GB or 8 GB LPDDR4-3200 SDRAM of memory; wireless support of 2.4 GHz and 5.0 GHz IEEE 802.11ac wireless, Bluetooth 5.0, BLE microcomputers were chosen for the hardware background.

CONTENTS

LIST OF ABBREVIATIONS

ATM - Asynchronous Transfer Mode

BLE - Bluetooth Low Energy

DHCP - Dynamic Host Configuration Protocol

FFD - full-featured devices

IaaS - Infrastructure as a Service

IIoT - Industrial Internet of Things

IoT – Internet of Things

IP – Internet Protocol

IPv4 - Internet Protocol version 4

IPv6 - Internet Protocol version 6

LAN - Local Area Network

LED - Light-emitting diode

LPWAN - Low-power wide-area network

MAC - Media Access Control

NAT - Network Address Translation

NFC - Near field communication

PaaS - Platform-as-a-Service

PAN - Personal Area Network

PLC - Power Line Communication

QoS - Quality of service

RAM – Random Access Memory

RFD - reduced function devices

RFID - Radio Frequency Identification

SaaS - Software-as-a-Service

TCP - Transmission Control Protocol

WAN - Wide Area Network

6LoWPAN - IPv6 over Low power Wireless Personal Area Networks

INTRODUCTION

Actuality of theme. Modern information technologies permeate all spheres of public life. The Internet of Things (IoT) is the latest stage in a long and ongoing revolution in computing and communications. IoT is a term used to describe a growing set of interconnected smart devices, from home appliances to tiny sensors. The Internet of Things is gaining more and more rapid development and is being implemented in many spheres of domestic, economic, industrial and social life. Internet of Things technologies are increasingly being used locally. They are a necessary condition for the development of smart devices and even cities.

However, technology, even one that is developing rapidly, can still be called unfinished, or raw. One way to improve the technical aspects of the Internet of Things is to implement Cloud Computing, among which we single out Fog Computing.

The purpose and objectives of the study. Analysis of the architecture, model, and principle of operation of the Internet of Things. Carrying out a comparative analysis of the characteristics of protocols and data transmission technologies. Consideration of Fog Computing, their comparative characterization with Cloud and Boundary Computing, and analysis of the implementation of the Internet of Things.

To achieve this goal, the following scientific problems are solved.

1. To reveal the essence of the concept of the Internet of Things, to distinguish the positive and negative aspects of technology.
2. Analyze Fog calculations, and their differences from other types of calculations.
3. Analyze protocols and technologies using Fog Computing to implement things on the Internet.

The object of study is Internet of Things and its architectures, protocols and characteristics.

The subject of research is Fog Computing and it’s connection with other types of Computing’s and Internet of Things.

Research methods. This paper presented an elementary platform of Internet of Things based on Cloud-Native technology and 3 network architectures based on the LoRaWAN protocol. Raspberry Pi 4 and Raspberry Pi Zero microcomputers were chosen for the hardware background.

The practical significance of the results obtained. Materials of the diploma work are recommended for use in research and practical activities on the planning of Internet of Things systems with the participation of Cloud Computing, as well as architectures and platforms involving Cloud Computing in the Internet of Things.

Approbation of the obtained results. The main provisions of the work were reported and discussed at the following conferences:

Scientific and practical conference "Problems of operation and protection of information and communication systems", Kyiv, 2022.

CHAPTER 1
INTRODUCTION TO THE CONCEPT AND GENERAL PROVISIONS OF THE INTERNET OF THINGS AND CLOUD COMPUTING

1.1. The concept and definition of the Internet of Things

The Internet of Things (IoT) is the networked integration of any devices (things) to enhance their usefulness. The finest example is a "smart house" system that can maintain a pleasant temperature, humidity, and other environmental parameters on its own. Special sensors monitor current performance, and the system subsequently switches on the air conditioner, thermostat, humidifier, or other equipment based on your preferences.

Kevin Ashton, a "technology pioneer," coined the term "Internet of Things." Ashton explored RFID (Radio Frequency Identification) in the late 1990s. This technology allows you to attach little tags to things that hold crucial information and read them from afar.

RFID tags can be found on items at stores, for example. A little sticker or tag enclosed in a plastic container. It allows, for example, to prevent theft in any form: when a product with an active tag approaches the exit sensor, an alert sound.

While working at Procter & Gamble in 1999, Kevin Ashton recommended to his bosses that they employ RFID tags to improve their supply chain management system. He coined the phrase "Internet of Things" to describe the concept.

The Internet of Things is a fairly broad idea. There is no definitive list of instruments that can be utilized with this method. These can be domestic equipment, such as a washing machine that can be operated remotely or a refrigerator that can create a shopping list and place an order for delivery. Wearable gadgets, such as fitness trackers and smart watches, are another alternative. Cars and other vehicles with an autopilot system that can drive itself are included in the Internet of Things [1].

The device may connect to the Internet or "cooperate" with other devices nearby. This is how "smart" house or "smart" city systems are created.

Devices designated as Internet of Things often have four technologies: an identification, sensors, communication tools with other devices, and an embedded computer.

As an identification, RFID tags, QR codes (those black and white squares that practically every modern phone can read), or other technologies are utilized. The instrument might have its own name thanks to the label.

Gauges and sensors are required to collect data from the environment. This is how a fitness tracker, for example, reads information about a person's pulse. Bluetooth or Wi-Fi can also be used to receive data from other devices and the network.

Finally, all received data is processed and programs are launched on an embedded computer. It might be extremely sophisticated, such as controlling the autopilot in a contemporary automobile, or quite simple [1].

Because of recent breakthroughs in communications and sensor technology, the Internet of Things (IoT) has been rapidly increasing. Interfacing every device with the internet appears challenging, but Internet of Things will radically impact our lives in the near future. The massive data captured by the Internet of Things (IoT) is regarded to have great corporate and social value, and various data mining algorithms can be used to extract hidden information from raw data.

Thousands of businesses, scientific, government, and private computer networks make up the contemporary Internet. The IP protocol is used to connect networks with diverse architectures and topologies. Each Network member (or group of members) is given a permanent or temporary IP address (dynamic).

Similarly, today's Internet of Things is made up of several loosely linked networks, each of which addresses its own set of issues. Several networks, for example, can be implemented simultaneously in an office building to operate air conditioners, heating systems, lighting, security, and other equipment. These networks can operate under a variety of standards, making merging them into a single network a difficult undertaking. Furthermore, the present (fourth) version of the Internet Protocol (IPv4) only allows for 4.22 billion addresses, resulting in address depletion. While not every item that connects to the Internet need a unique IP address (but does require a unique identification), address shortages may become a limiting concern as the Internet of Things grows. IPv6, the sixth

version of the protocol, will assist to significantly alleviate the problem, allowing each person on the planet to utilize more than 300 million IP addresses [2].

By 2023, it is estimated that the globe will have between 70 and 100 billion networked devices, and the IPv6 protocol's addressing capabilities will allow nearly every object on the Internet to be identified.

The Internet of Things is based on the technologies listed below.

Identification methods

Even if it is not linked to the Internet, every object in the physical world participating in the Internet of Things must have a unique identification. For automatic item identification, a variety of currently existing technologies can be used: radio frequency (a radio frequency label is affixed to each object), optical (barcodes, Data Matrix, QR codes), infrared tags, and so on. However, effort must be done to standardize IDs of various sorts to assure their uniqueness [3].

Measuring

The purpose of measuring instruments is to guarantee that information about the external environment is transformed into data that can be sent to processing devices. Separate temperature and light sensors, as well as complicated measurement systems, can be used. To achieve measuring instrument autonomy, alternative energy sources (solar batteries) should be used to deliver power to the sensors, rather than wasting time and money recharging or replacing batteries.

Media of communication

For data transmission, any of the available technologies can be employed. When using wireless networks, extra care is taken to improve data transfer dependability. Because many objects (such as vending machines, ATMs, and other devices) are connected to the power grid, data transfer technology across power lines is actively employed when using wired networks.

Tools for data processing

In 2023, the estimated 70 billion or more gadgets linked to the Internet will create 94 billion gigabytes of data. This is almost eight times the quantity of digital data available globally in the 2010s. As a result, Microsoft believes that the fundamental component of the

Internet of Things is cloud services that provide high bandwidth and can respond fast to specific events, rather than sensors and data transmission methods (for example, be able to find out from the readings of sensors that the house has been in the house for five minutes). There is no one there, and the front door is open). Fog computing will also aid in the management of large amounts of data, complementing rather than competing with cloud computing.

Devices for Execution

These are devices that can transform digital electrical signals from operational information networks. For example, a smartphone must have a proper gadget in order to switch on the house's heating system. Actuators and sensors are frequently structurally integrated [3].

1.2. Architectures, protocols, characteristics, schemes and telecommunication technologies of the Internet of Things

Architecture of the Internet of Things

IoT connects millions of smart objects, which leads to increased data traffic and the need for large processors and storage. Based on the above, IoT faces problems in the quality of service, data protection and security. Thus, the IoT architecture must take into account a number of issues, such as compatibility, scalability, QoS, reliability, and so on. However, each of the proposed architectures has a number of common shortcomings and does not cover all the features of IoT, which are summarized below:

a. Distributor: The IoT model was probably developed in a highly distributed environment, where data can be collected from different sources and, accordingly, processed by different smart objects in a distributed process.

b. Compatibility: IoT devices from different manufacturers need to communicate with each other to achieve common goals. Protocols and systems must also be designed in such a way that intelligent devices from many manufacturers allow the interactive exchange of tangible data.

c. Scalability: Billions of objects are expected to connect to any Internet of Things environment. Therefore, programs and systems running in these environments must be able to process and process vast amounts of data.

d. Resource shortages: both computing and energy are extremely scarce resources.

e. Security: User inertia and a sense of control and control by an unknown external device can seriously impede IoT deployment [4].

To address these issues, many researchers are following a multi-layered architecture for the IoT infrastructure. In all proposed IoT architectures, similar techniques, functions and services will be grouped into one level, which will contribute to the development and improvement of the architecture of each level in the future. There is no global consensus on the IoT architecture, so many researchers suggest different IoT architectures. As far as we know, after extensive research into IoT architecture models, we have found that the best model for the elements that make up the environment is the "three-based architecture" model described in. This architecture consists of the following three layers:

a. IoT layer: This level contains all smart devices, entities and end users in the IoT system.

b. Fog layer: all fog nodes are located in this layer.

c. Cloud level: All distributed cloud servers are located at this level, where these servers consist of multiple processor units, such as a high-capacity server rack, or can be a huge server with multiple processing cores.

The simplest architecture is the three-tier architecture. This was introduced in the early stages of research in this area. It has three levels, namely the detection level, network and application [4].

1. Perception layer is the physical level that sensors have for detecting the environment and collecting information. Detects some physical parameters or identifies other intelligent objects in the environment.

2. The network layer is responsible for connecting to other smart things, network devices and servers. Its functions are also used to transmit and process sensor data.

3. The application layer is responsible for providing program-related services to the user. It identifies a variety of programs in which you can deploy the Internet of Things, such as smart homes, smart cities, and smart healthcare.

At each level, the nodes are grouped into domains, where a single IoT domain consisting of Nodes-Fog-Cloud agents can execute a program. The following is a computing node and a cloud server for communicating and interacting with each other; first, the IoT node transmits its tangible data directly to the nebula node belonging to its domain program. As a result, the fog node processes the received data directly or sends it to another fog node or cloud server in the same domain to return a response to the associated IoT node. This step reduces the service delay of the IoT5 node when it responds to any request, it comes from the location of the fog layer, which allows its nodes to process most requests from the IoT level. The following sections present the architecture of each level in the architecture model on three bases [4].

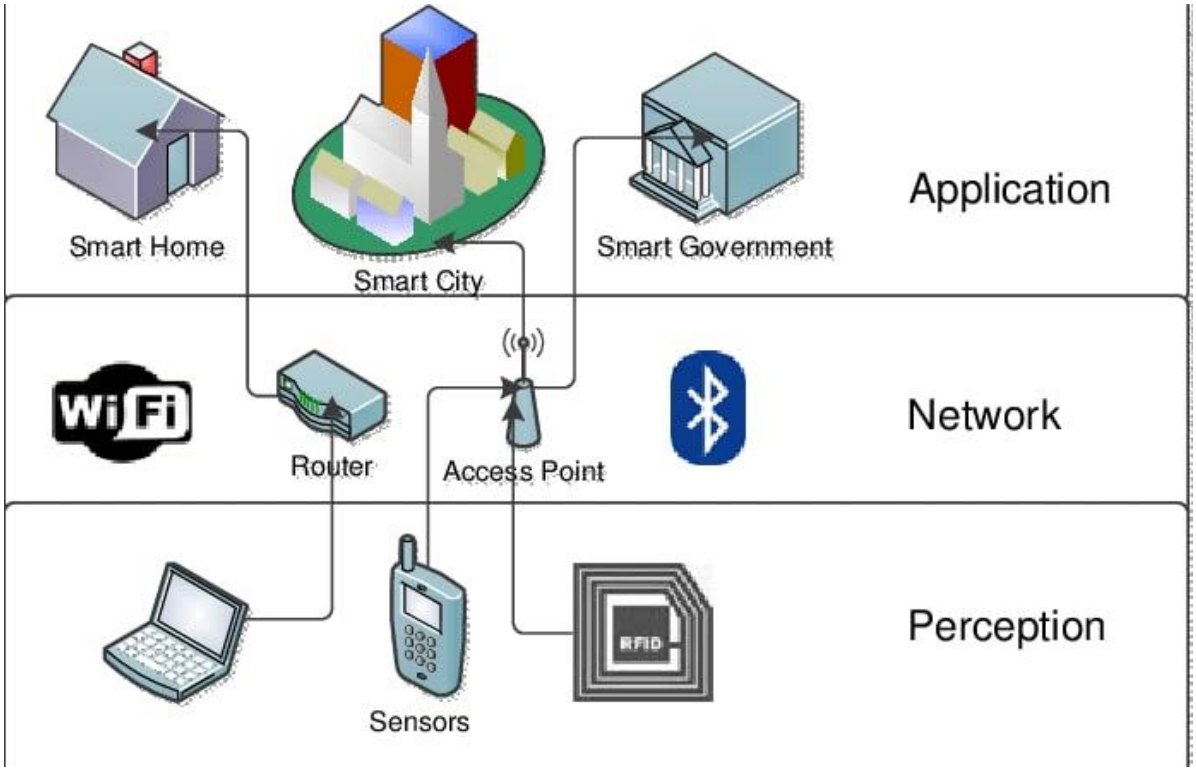

Fig. 1.1. Three based architecture layer of Internet of Things [4]

Five-layer architecture

The three-tier architecture defines the basic idea of the Internet of Things, but this is not enough for IoT research, as research often focuses on subtle aspects of the Internet of Things. That is why the literature offers a much more multi-layered architecture. One of them is the five-level architecture, which also includes processing levels and business. The five levels are the levels of perception, transportation, processing, application and business. The role of levels of perception and applications is the same as that of three-level architecture. Outline the function of the other three layers.

1. The transport layer transmits sensor data from the detection level to the processing layer and vice versa over networks such as wireless networks, 3G, LAN, Bluetooth, RFID and NFC.

2. The processing layer is also called the middleware level. It stores, analyzes and processes huge amounts of data from the transport layer. It can handle and provide a wide range of services to the lower strata. It uses a number of technologies such as databases, cloud computing and large data processing modules.

3. The business layer manages the entire IoT system, including applications, business and profit models, and user privacy [5].

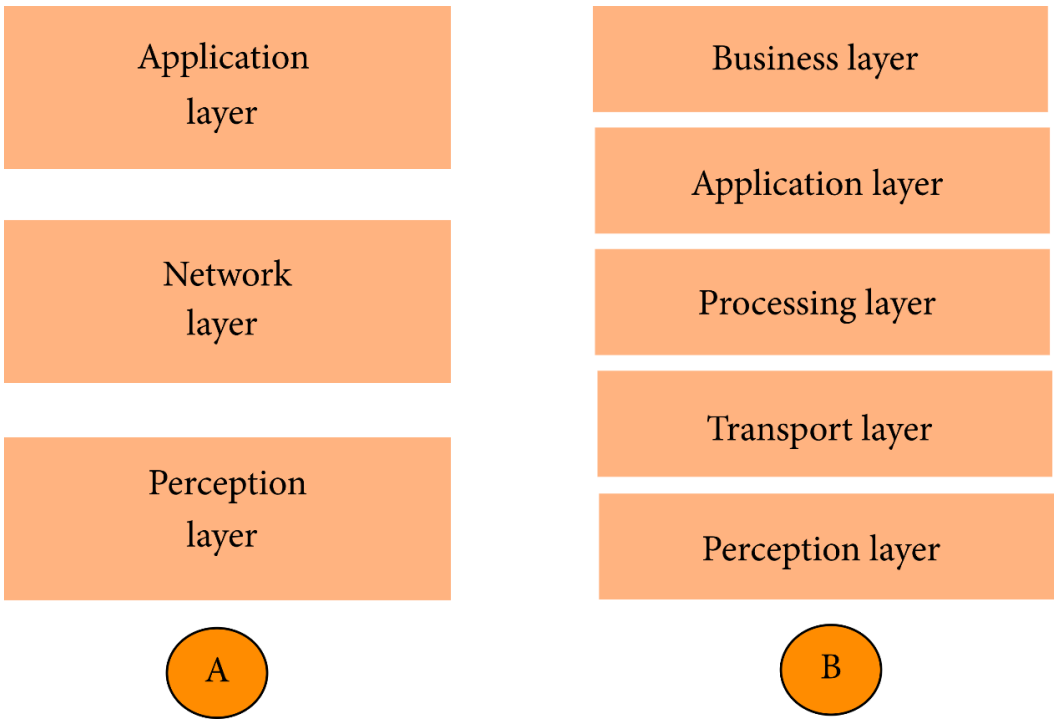

Fig. 1.2. Three and Five-layer architecture of Internet of things [5]

The IoT paradigm consists of a number of functional blocks that facilitate various functions of intelligent objects, such as detection, activation, identification, control, and communication. Figure 1.2. shows these blocks with brief explanations in the following sections:

Device. Smart devices are the basic units of the IoT system, where they can perform a number of operations, such as detection, monitoring, control and operational activities. They can also share data with applications and other smart servers. All IoT devices must be equipped with many interfaces to connect to other smart devices consisting of interfaces for Internet connection, touch I / O, audio / video, memory and storage. IoT devices vary by application. Such applications can be smart watches, wearable sensors, cars, industrial machines, LED lamps and more [5].

Services: There are many programs that use the Internet of Things, from office and home automation to production lines and product tracking. Thus, special IoT services must be used to improve and accelerate the development of IoT applications. implementation. These services

related services, asset modeling services, information aggregation services, asset discovery, asset management, joint services, ubiquitous services, data analysis and data transmission.

Control: a key feature of the IoT device that distinguishes it from traditional devices that can be controlled and controlled by mechanical buttons or switches, with remote control with or without human intervention. In addition, these tools can exchange data with each other in order to make a decision at a later stage.

Security: Data on networks, especially wireless networks, is subject to a large number of attacks, such as denial of service, forgery, eavesdropping, etc. features such as privacy, authorization, authentication, data security, content integrity, and message integrity.

Application: The application layer provides interfaces for Internet of Things users that allow them to control and control various aspects of IoT applications. In addition, they allow users to analyze and visualize the state of the IoT system at any time and in any place to take appropriate action [6].

The main components of IoT devices

IoT systems, as mentioned earlier, consist of devices and applications that must have the main components to communicate with each other, as shown below:

1. Identification (ID): each object in the IoT system must have a unique identifier; The identifier is assigned to the entity based on traditional parameters, such as the universal product key, MAC ID, IPv6 ID, or other custom method.

2. Metadata. Metadata contains information about each device in the IoT system, such as device model, ID, version, hardware, serial number, and date of manufacture.

3. Security checks: Similar to the "friends list" on Facebook, because the owner of the device may limit the type of devices connected to his device.

4. Service Discovery: This feature allows each IoT device to store data from all other smart devices on the network in a specific directory. It is very important to keep these directories up to date in order to receive information about new devices that have recently joined the IoT network.

5. Connection Management: Allows any Internet of Things device to initiate, update, and disconnect from itself and other devices. It also maintains a list of the types of devices to be connected to, according to the type of services they provide and based on human settings. For example, a light sensor can connect to a light control device.

6. Composition of the service: This component allows interaction between intelligent objects and is designed to provide the best integrated services to users. To achieve these goals, the detection service tries to find the right service provided by the smart object to use later. He is also responsible for processing data received from various objects to offer the best solution for the user [7].

The Internet of Things (IoT) consists of smart devices that communicate with each other. This allows these devices to collect and exchange data. In addition, IoT now has a wide range of applications for life, such as industry, transportation, logistics, healthcare, a smart environment, a personal gaming robot for the community, and information about the city. Smart devices can have a wired or wireless connection. As for the wireless Internet of Things, the main problem is that you can use many different wireless communication technologies and protocols to connect a smart device, such as Internet Protocol version 6

(IPv6), low-power wireless personal area networks (6LoWPAN), ZigBee, Bluetooth Low Energy (BLE), Z-Wave and Near Communication (NFC). These are standard short-range network protocols, while SigFox and Cellular are low-power wide area networks (LPWANs). standard protocols. This article will try to look at different communication protocols on the Internet of Things [7].

IPv6 and IPv4

IPv6 is the next generation Internet protocol, and the Internet is still migrating from IPv4. Public IPv4 addresses have been exhausted, and various methods, such as Dynamic Host Management Protocol (DHCP), Network Address Translation (NAT), and subnets, have been proposed to slow the depletion rate of IPv4 IP addresses. .

In practice, IPv6 is much more than an extension of IPv4 addressing. IPv6, first defined in RFC 2460, is a complete implementation of the network layer stack of TCP / IP protocols and includes much more than simply extending the address range from 32 bits to 128 bits (a mechanism that allows IPv6 to assign addresses to all devices in the world). the coming decades).

The technical work of the Internet will remain the same for both versions of IP, and it is likely that in the future both versions will work simultaneously on networks. Today, most networks that use IPv6 also support IPv4 and IPv6 addresses [8].

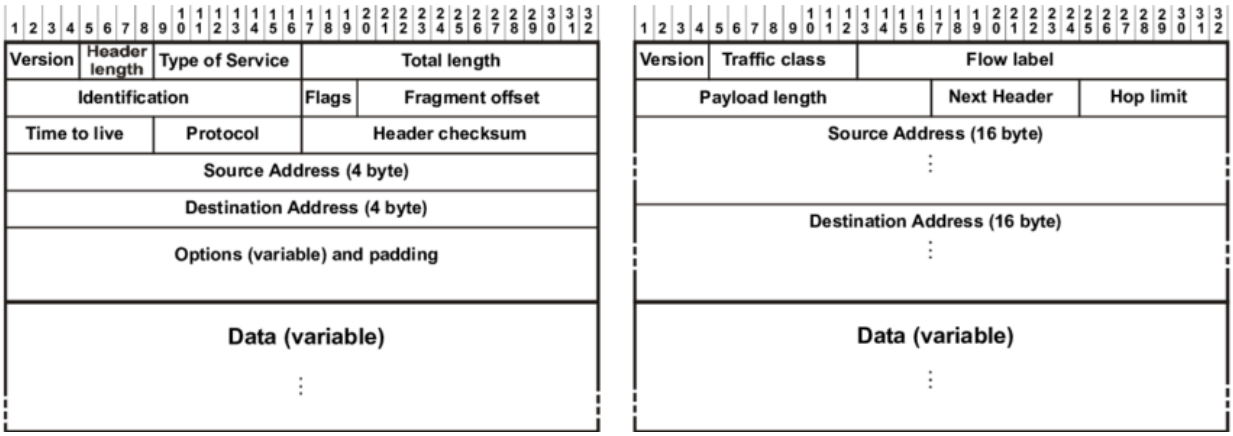

Fig. 1.3. Header structure for IPv4 (left) and IPv6 (right) packets [8]

IPv4 uses 32-bit (4-byte) decimal addresses with dots, for example 192,168,252.64, all records are decimal numbers - zeros can be omitted at the beginning. The address consists

of a network and a node, which depend on the address class. Different classes of addresses are defined: A, B, C, D or E depending on the first few bits. The total number of IPv4 addresses is 2^{32} = 4,294,967,296. NAT can be used to extend these restrictions to the address. The length of the IPv4 header varies from 20 to 60 bytes, depending on the selected IP settings. IPSec support is optional, and settings are embedded in the header fields (before each transport header).

IPv6 uses 128-bit (16-byte) addresses with a hexadecimal entry (ie each entry corresponds to 4 bits), for example 3FFE:F200:0234:AB00. The base architecture is 64 bits for the network number and 64 bits for the host number. Part (or part) of a number of IPv6 addresses often comes from a MAC address or other interface ID. The total number of IPv6 addresses is $2^{128} = 3.4*10^{38}$. NAT support is not provided.

The IPv6 header has a fixed length of 40 bytes and has no IP header settings. IPSec must be supported, and the settings are supported by extension headers (there is a simpler header format). Extension headers are AH and ESP (unchanged from IPv4), phased, routing, snippet, and target [8].

IEEE 802.15.4 and ZigBee

The IEEE 802.15 team defined physical layer (PHY) and medium access level (MAC) for WPAN connections with low complexity, low power consumption, and low bit rate. The IEEE 802.15.4 standard, approved in 2003 and amended several times over the following years, contributes to all of these goals, and many relevant products are already available on the market, albeit as a development kit and not as a true end product.

The IEEE 802.15.4 physical layer requires the use of one of three possible unlicensed frequency bands:

868.0-868.6 MHz: used in Europe and allows one communication channel (versions released in 2003, 2006, 2011);

902-928 MHz: used in North America, up to ten channels (2003), extended to thirty (2006);

2400-2483.5 MHz: used worldwide with up to sixteen channels (2003, 2006).

IEEE 802.15.4e, which was finally approved in 2012, defines a modification of the MAC to the existing standard 802.15.4-2006. The channel uses a jumping strategy to improve support for industrial markets and increase resilience to external interference and constant multi-beam attenuation [8].

The IEEE 802.15.4 family provides low-speed data connections in the personal operating space; this is usually 10 to 100 m. Full network support for battery-powered nodes can be achieved by classifying devices into two different types: full-featured devices (FFDs) and low-performance devices (RFDs). The IEEE 802.15.4 network must include at least one FFD that acts as a PAN coordinator for special (but not centralized) functions, while all other FFDs must form the basis of a wireless sensor network (WSN); RFDs, which are typically designated as "leaf" nodes in a tree spanning WSN, perform simple detection tasks, not network. RFD can communicate with only one FFD, while FFD can communicate with both RFD and FFD.

In the late 2000s, a consortium of hundreds of companies agreed to adopt an industry standard called ZigBee based on the current IEEE 802.15.4 specification; The name was inspired by the social behavior of bees, which together solve complex problems. Using compatibility, ZigBee provides multi-jump messaging and provides logical network, security, and application management capabilities in addition to the referenced IEEE 802.15.4 standard by defining top-level protocol stack levels from network to program. In addition, ZigBee defines application profiles, descriptions of device configurations based on templates, each of which specializes in working in a common shared and distributed application. In addition to technical aspects, one of the main tasks of the ZigBee Alliance is to ensure interoperability between devices from different manufacturers, thus expanding their application [8].

Bluetooth and BLE

Bluetooth is a standard replacement wired communication protocol designed primarily for low power consumption and short-range communication. Transmission range depends on performance. The specifications were formalized by the Bluetooth Special Interest Group (SIG). SIG was officially established by Ericsson, IBM, Intel, Toshiba and Nokia in 1998: it now has more than 30,000 members worldwide. While Bluetooth 3.0,

introduced in 2009, supports a data rate of 25 Mbps with a transmission range of 10 meters, the latest Bluetooth 5.0, introduced in 2016, has increased the data rate and transmission range to 50 Mbps and 240 meters. At the top of the physical layer, channel-level services are available, including media access, connection establishment, error handling, and flow management. The top logical connection management and adaptation protocol provides data channel multiplexing, fragmentation, and reassembly of large packets. Additional upper tiers are the Generic Attribute Protocol, which allows efficient collection of data from sensors, and the shared access profile, which allows you to configure and operate in various modes, such as advertising or scanning, as well as initiating and managing a connection.

Version 4.0 of the Bluetooth kernel specification (aka "Bluetooth Smart") was adopted in 2010. Bluetooth 4.0 includes the classic Bluetooth, Bluetooth High Speed and Bluetooth Low Energy (BLE) protocols. Bluetooth is based on high-speed Wi-Fi, while classic Bluetooth consists of outdated Bluetooth protocols. BLE, formerly known as Wibree, is a subset of Bluetooth 4.0 with a completely new set of protocols for quickly creating simple links. It is designed for very low power applications that run on a tablet battery. The design of the chip allows two implementations: dual mode and one mode.

Starting with version 4.2, Internet of Things-oriented features have been introduced in Bluetooth:

secure low power connection with packet extension (v4.2);

channel layer data protection (v4.2);

IP support profile (v6.0), ready for Bluetooth Smart Things to support connected homes (v4.2);

offline services such as location-based navigation for low-power Bluetooth connections (v5.0) [8].

BLE uses a low-power radio that can run much longer (up to years) than previous versions. Its range (about 100 m) is 10 times longer than classic Bluetooth, and the delay is 15 times less. BLE can operate with a transmission power of 0.01 to 10 mW. Thanks to these features, BLE is a good candidate for IoT applications. The BLE standard was quickly developed by smartphone manufacturers and is now available on most smartphone models.

The relevance of this standard has been demonstrated in communication between vehicles as well as in the WSN.

Compared to ZigBee, BLE is more efficient in terms of the ratio of power consumption to transmission step by step. BLE allows devices to act as a master or slave in a star topology. For the detection mechanism, slaves send ads through one or more dedicated advertising channels. To detect how subordinate, these channels are scanned by the master. If no communication is in progress, the devices are in the Sleep state.

The LoWPAN Adaptation Layer

Low-power wireless personal area networks (WPANs) have special features that set them apart from previous connection-level technologies. These include limited packet size (up to 127 bytes for IEEE 802.15.4), different address lengths and low bandwidth. These features require an adaptation level that aligns IPv6 packets with IEEE 802.15.4 specifications. The IETF 6LoWPAN working group developed this standard in 2007. 6LoWPAN is a specification for mapping services required to support IPv6 over low-power WPANs. The standard provides header compression to reduce transmission overhead, fragmentation to meet the IPv6 MTU requirement, and channel-to-channel forwarding to support multi-jump delivery. Typically, the purpose of 6LoWPAN is to transmit a small IPv6 datagram over a single IEEE 802.15.4 transition [8].

1.3. Advantages and disadvantages of the Internet of Things

Benefits of IoT

These patterns are now clear. Adding internet connectivity to household appliances used to be tough, but the complexity and expense of doing so has substantially lowered in recent years. Arduino computers may now transform any household object into a smart gadget. And Amazon's technology appears to have the potential to dramatically speed up the creation of IoT devices. During a press conference, Amazon's developer revealed how simple it is to transform a regular hair dryer into a "smart" one by utilizing a special Amazon chip called the Alexa Connect Kit. If you buy it straight from Amazon, the hair dryer will connect to your home network and wait for you to give voice commands. This technology

demonstrates that the cost of placing a computer in a home object will be so low that manufacturers will have an easier time connecting anything else to the Internet. Our lives are already being made easier by "smart devices." In the future, you'll only be able to use the voice command to make the microwave reheat up your lunch if you're in another room. However, these gadgets will mostly be utilized for marketing and consumer tracking. They have the ability to construct their own market rationale. Gadgets that can't connect to the Internet will eventually be harder to come by than those that can [9].

Communication

Communication between devices, also known as machine-to-machine (M2M) communication, is encouraged by the Internet of Things. As a consequence, physical assets may remain linked, allowing for full transparency with less effort and higher quality.

Control and automation

Because of the connectivity and management of physical things in a digital and centralized fashion with the wireless infrastructure, there is a lot of automation and control at work. Machines can interact with one other without the need for human involvement, resulting in a faster and timelier exit.

Monitoring

Monitoring is the second most evident benefit of IoT. You may gain extra information that was previously difficult to obtain by understanding the exact number of supplies or the air quality in your house. For instance, if you anticipate you'll run out of milk or printer ink soon, you may avoid making another trip to the shop. In addition, keeping track of a product's shelf life may and will increase safety.

Money

The most significant benefit of IoT is cost savings. The Internet of Things will grow in popularity if the cost of labeling and monitoring devices is less than the money saved. IoT is typically beneficial to individuals in their daily lives since gadgets interact efficiently with one another, saving energy and money. This allows data to be exchanged across devices and then translated as needed, making our systems more efficient.

A higher standard of living Each use of this technology results in enhanced comfort, convenience, and superior handling, all of which improve life quality.

Weakness of the Internet of Things

Security issue

The issue is that these gadgets' business models do not provide the same level of security as regular Internet devices. Apple has an incentive to keep your phone secure by releasing security upgrades. The reason for this is because the iPhone is relatively expensive, and the Apple brand values its reputation and goes to great lengths to safeguard users from viruses and bugs. Budget home appliance makers, on the other hand, lack the necessary experience or motivation. That is why "poor security" has become synonymous with the Internet of Things. With the conveyance of all this IoT data, the risk of losing privacy increases. How well will storage and transmission be encrypted, for example? Do you want your neighbors or bosses to know what medication's you are using on or how much money you have? Consider a well-known hacker who alters your prescription medications. Or if the merchant automatically substitutes an equivalent product that you are allergic to, has a flavor you dislike, or is out of date. As a consequence, customer safety is ultimately in their hands when it comes to controlling all forms of automation. A lot of information is available since all household appliances, industrial equipment, utilities such as water and transportation, and many other gadgets are connected to the Internet. Normally, this information is used to combat hackers. Unauthorized attackers would be exceedingly dangerous if they gained access to personal and private information [9].

Compatibility

Because devices from many manufacturers are interconnected, there is a concern of labeling and monitoring compatibility. Although technological issues can be mitigated if all manufacturers agree on a uniform standard, they still remain. We now have Bluetooth-enabled devices, but even with this technology, there are compatibility concerns! People may purchase products from a specific manufacturer due to compatibility issues, resulting in a monopoly on the market.

Complexity The Internet of Things (IoT) is a vast and complicated network. Any software or hardware problem might have catastrophic ramifications. Even a brief power loss can be quite inconvenient.

Workers employed on a small scale. As a result of the automation of daily chores, unskilled workers and helpers may lose their jobs. This may result in societal unemployment. This is a problem that arises with the introduction of any technology and is easily remedied via education. Of course, as daily operations become more automated, there will be less demand for human resources, particularly for employees and less skilled personnel. This may result in societal unemployment [9].

1.4. Scenarios of implementation in modern world

IoT affects all areas of our lives. IoT-enabled applications can be found in several scenarios, including home and building automation, smart cities, smart grids, Industry 4.0, and smart agriculture. In each of these areas, a common (IP-oriented) stack of communication protocols allows you to create innovative applications. In this section, we provide a brief overview of possible applications in these areas.

IoT-compliant programs

Automation of houses and buildings

As the smart home market grew and developed, more and more home automation applications appeared for a specific audience. As a result, several separate vertical market segments were created. Typical examples of increasingly common applications are home security, energy efficiency and energy saving. Encouraged by innovations in lighting and room management, IoT helps develop an endless number of home automation applications. For example, a typical example of the field of home automation that will be developed in the context of IoT is healthcare, namely IoT-enabled solutions for less mobile (including the elderly, which are especially important for the aging population) and people with disabilities or chronic diseases for patients (eg remote monitoring of health and air quality). In general, building automation solutions are beginning to converge and move from modern luxury, security and convenience applications to a wider range of applications and interconnected solutions; this creates market opportunities. Although modern smart home solutions are fragmented, IoT is expected to lead to a new level of interoperability between commercial buildings and building automation solutions.

Smart cities

Cities are complex ecosystems where quality of life is an important factor. In such an urban environment, people, companies and public authorities face special needs and requirements in areas such as health, media, energy and the environment, security and public services. The city is increasingly perceived as the only "organism" that needs to be effectively monitored so that citizens are accurately informed. IoT technologies are needed to collect data on the state of the city and disseminate it to citizens. In this context, cities and urban areas are critical when it comes to shaping the demand for advanced IoT-based services [8].

Smart grids

A smart grid is an electrical grid that includes a number of operating systems, including smart meters, smart devices, renewable energy sources, and energy-efficient resources. Wiring (PLC) is associated with the use of existing electrical cables for data transmission and has long been studied. Electricity suppliers have been using this technology for years to send or receive data (in limited quantities) from the existing grid. Although the PLC is mostly limited by the type of propagation medium, it can use wires in the distribution network. According to EU standards and laws, electric companies can use PLCs for data transmission with low data rates (data rates less than 50 Kbps) in the frequency range 3-148 kHz. This technology opens up new possibilities and new interactions between people and things in many programs, such as intelligent metering and electricity reporting services. This allows you to control, manage and automate PLCs in large systems located in relatively wide areas, such as smart city and smart grid scenarios. In addition to PLC, you can use authorization technologies that can improve intelligent automation processes, such as the Internet of Things. For example, the use of PLC technology in industrial scenarios (for example, remote control in automated and manufacturing companies) opens the way to the Internet of Things. Many applications have been enabled due to the ability of PLC technology to recover from network changes (in terms of fixes and improvements, physical removal and transmission functionality), reducing signal loss. However, it is well known that power lines are far from ideal for data transmission (due to internal differences in location, time, frequency range and type of

equipment connected to the line). As a result, there is growing interest in the joint adoption of IoT and PLC paradigms to improve communication reliability. This has led to the proposal to use small, resource-intensive tools (namely IoT) with integrated computing capabilities and standard Internet solutions (as proposed by Internet standards organizations such as IETF, ETSI and W3C). Such systems can be key components in the implementation of future smart grids [8].

Industrial Internet of Things

The Industrial Internet of Things (IIoT) describes the Internet of Things as it is used in industries such as manufacturing, logistics, oil and gas, transport, energy / utilities, mining and metals, and aviation and others. These industries account for the majority of gross domestic product in the G20. IIoT is still in its infancy, similar to where the Internet was in the late 1990s. Although the development of the consumer Internet has provided important lessons over the past two decades, it is unclear to what extent this training is applicable to the Internet of Things, given its unique scope and requirements. For example, real-time responses are often crucial in manufacturing, energy, transportation, and healthcare: real-time online today is usually a few seconds, while real-time on industrial machines is less than a millisecond. Another important aspect is reliability. The current Internet embodies a "best effort" approach that provides acceptable performance for e-commerce or human interaction. However, failure of the grid, air traffic control system or automated installation over the same period of time would have much more serious consequences. Much attention has been paid to the efforts of large companies such as Cisco, GE and Huawei, as well as government initiatives such as Industrie 4.0 in Germany. For example, GE announced that it achieved revenue growth of more than $ 1 billion in 2014, helping its customers improve device performance and business operations through IIoT capabilities and services. The German government supports Industrie 4.0, a multi-year strategic initiative that brings together leaders from the public and private sectors, as well as academia, to develop a comprehensive vision and action plan for the use of digital technologies in Germany's industrial sector. Other European countries also have their own IIoT-focused industrial transformation projects, such as Smart Factory (Netherlands), Industry 4.0 (Italy), Future Industry (France) and others.

China has also recently launched its Made in China 2025 strategy to promote the integration of digital technologies and industrialization.

As IIoT accelerates, one of the biggest bottlenecks is the inability to exchange information between smart devices that can speak different "languages". This lack of communication is due to the variety of protocols used at the factory level. Thus, although you can install a sensor on your computer to collect data, transmitting information over a network and, ultimately, "talking" to other systems is a bit more difficult. Thus, standardization is a key element of IIoT. The potential impact of IIoT is huge. Operational efficiency is one of the most important benefits, and first users are focusing on these benefits. For example, with the introduction of automation and more flexible production technologies, manufacturers can increase their productivity by up to 30%. In this context, three IIoT capabilities need to be explored: sensor-driven computing: converting sensitive data into deep data (using industry analysis described below) to which operators and systems can respond; industrial analytics: conversion of data from sensors and other sources into practical knowledge; application of intelligent machines: integration of sensor devices and intelligent components into machines [8].

Intelligent control

Modern agriculture is facing enormous challenges as it seeks to build a sustainable future in different parts of the world. Such issues include population growth, urbanization, environmental degradation, increasing animal protein consumption, population aging and changing food preferences due to migration and of course climate change. There is a need for the development of modern agriculture, characterized by the introduction of production methods, technologies and tools derived from the achievements of science, as well as the results of research and development. Precision farming or intelligent agriculture is the area with the greatest potential for digital development, but with the lowest prevalence of digitized solutions today. Agriculture is probably more important than ever in the next few decades. The use of environmental and ground sensors, weather monitoring, automation of more accurate application of fertilizers and pesticides (thus reducing the loss of natural resources) and the adoption of maintenance planning strategies can have enormous benefits. Smart farming is already becoming widespread through the use of new technologies such as

drones and sensor networks (for data collection) and cloud platforms (for data collection management). The range of technologies used in smart farming is as complex as the activities of farmers, producers and other stakeholders in the sector. There is a wide range of possible applications: fleet management, animal husbandry, fisheries, forestry, indoor urban management and much more. All the technologies involved revolve around the concept of IoT and are aimed at supporting farmers in decision-making processes through decision support systems. They contain real-time data at a level of detail that was previously impossible. This allows you to make better decisions, which leads to lower costs and increased efficiency. Communication technologies are key elements of intelligent agricultural applications. Wireless technologies are especially attractive because cables are significantly shortened and simplified. Various wireless standards have been set. They can be divided into two main categories depending on the transmission range:

- Short distance communication: including standards:

1. Wireless LAN used for Wi-Fi, namely IEEE 802.11
2. Wireless PAN for more widely used measurement and automation programs, such as IEEE 802.15.1 (Bluetooth) (IEEE, 2002) and IEEE 802.15.4 (ZigBee / 6LoWPAN) (IEEE, 2003). All of these standards use instrumental, scientific, and medical (ISM) radio bands, which typically operate in the 2400-2.4835 GHz band. Long-distance connectivity: Including the increasingly important sub-GHz IoT technologies, such as LoRA, in the 868-870 MHz band. They are looking for data rates (of the order of hundreds of kbit / s) for larger transmission ranges. Communication technologies can also be classified according to the specific application:

- environmental monitoring (weather control and geo-linked environmental monitoring)
- precision farming
- machine and process control (M2M communication)
- object automation
- tracking systems. [8]

1.5. Cloud Computing. Types of cloud computing

Models of Cloud Deployment

Private Cloud

Only one firm or group of organizations uses all private cloud resources. Both the client organization and the cloud service provider are in charge of this cloud computing deployment approach. Typically, such a feature is discussed during the contracting stage. When a corporation recognizes that it lacks the necessary professionals, it employs the remote administration service.

Community cloud

The service provider provides a cloud infrastructure for a group of customers that share a common objective, security policy, and set of requirements for getting the job done correctly. Multiple community organizations or a service provider can own and run a cloud.

Public cloud

Different users on the Internet can access and utilize the resources of such a cloud. Typically, a government, commercial, or academic institution manages and owns the cloud infrastructure. Public cloud services are utilized by both ordinary users and start-ups and major corporations with several locations.

Hybrid cloud

Two different cloud infrastructure models make up this concept. Even when they work together as a hybrid, they remain separate organizations with unique technologies. The firm sends data through it [10].

The basic argument is that renting is preferable to buying, that is, using a service rather than buying a thing. You may rent computer power, disk space, licenses, and other services from cloud solution providers through the Internet. The benefits of this strategy include efficiency and speed (the user pays just for the resources he requires and receives them within a few hours), as well as the ability to scale and expand in a flexible manner.

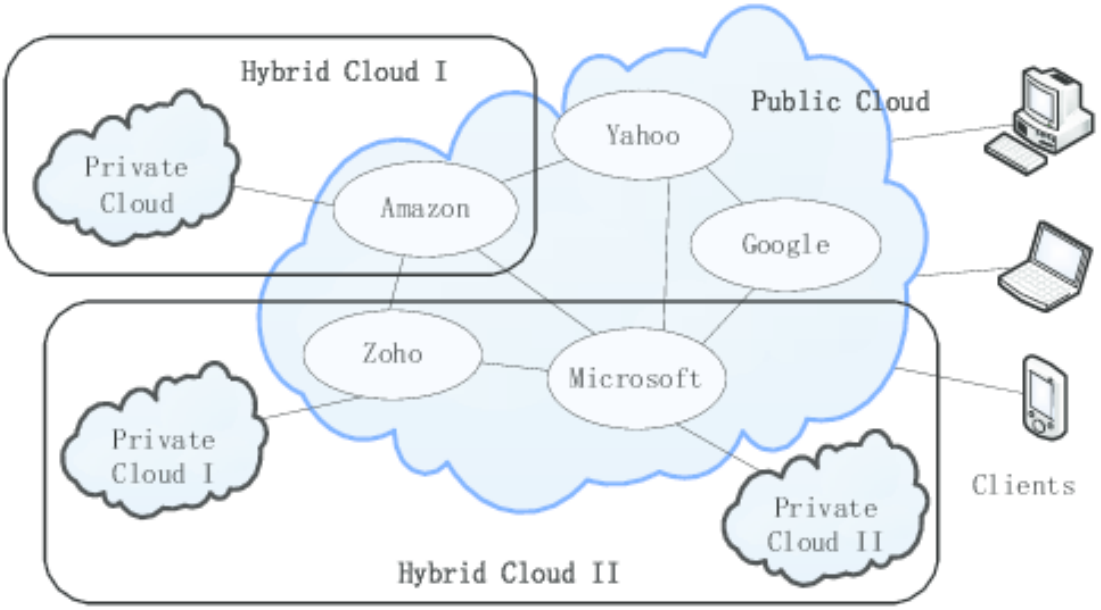

Fig. 1.4. Example of Cloud Computing [10]

The cloud presents a service-oriented approach between the business and the IT department, allowing IT to better meet the needs of today's fast-paced business reality. Cloud computing is a cutting-edge multipurpose solution, but it is still only a tool in the hands of IT experts. Cloud computing enables you to swiftly and precisely modify your IT infrastructure to fit business needs [10].

Without interacting with a representative of the service provider, the customer autonomously determines and adjusts computing demands, such as server time, speed of access and data processing, and the amount of stored data.

Universal network access; services are available to users over the data transmission network, independent of terminal equipment;

In resource pooling, a service provider pools resources to serve a large number of customers into a single pool for dynamic redistribution of capacity between customers in a constantly changing demand for capacity; customers control only the basic parameters of the service (for example, data volume and access speed), but the provider manages the actual allocation of resources to the customer (in some cases, customers can still control some of the allocation) [11].

Consumption accounting, in which the service provider automatically calculates the consumed resources at a certain level of abstraction and estimates the volume of services provided to consumers based on this data;

Elasticity, services can be provided, expanded, or narrowed at any time, without additional costs for interaction with the supplier, as a rule, automatically;

Cloud computing helps providers to achieve economies of scale by pooling resources and reducing costs by employing fewer hardware resources per customer than per-customer hardware provisioning and automating resource provisioning adjustment operations. for the purpose of a subscription service

From the consumer's perspective, these characteristics enable them to obtain services with a high level of availability (eng. high availability) and low risks of disability, as well as to ensure rapid scaling of the computing system due to elasticity, all without having to build, maintain, and upgrade their own hardware infrastructure.

The extensive availability of services and support for many types of terminal devices ensures convenience and diversity of access (personal computers, mobile phones) [11].

Models of Service

The extent of automation of the infrastructure's IT activities is determined by the service model. The following are some examples of cloud-based service delivery models:

Software-as-a-Service (SaaS) (SaaS) Gmail and Google Docs are two instances of cloud-based software as a service.

Platform-as-a-Service (PaaS) (PaaS) Google Apps, for example, offers online business apps that can be accessed using a browser and are hosted on Google servers.

Infrastructure as a Service (IaaS) is a kind of cloud computing (IaaS) Amazon, Microsoft, VMWare, Rackspace, and Red Hat are the industry leaders in IaaS. While some go beyond infrastructure, they all have the same purpose of selling fundamental computer services. And, while all cloud services are built on the notion of remote computing, this principle may be applied in a variety of ways. It all relies on the resource's purpose, user demands, and functioning. Software as a Service (SaaS) ("software as a service"), Platform as a Service (PaaS) ("platform as a service"), and Infrastructure as a Service (IaaS) ("infrastructure as a service") are the three most prevalent cloud use types [11].

Table 1.1

Difference between types of Models of Service

Traditional approach	Service approach to IT infrastructure management		
	IaaS	PaaS	SaaS
Install patches and updates throughout the program lifecycle	Install patches and updates throughout the program lifecycle	Install patches and updates throughout the program lifecycle	Install patches and updates throughout the program lifecycle
Download User Data	Download User Data	Download User Data	Download User Data
Installation of complex applications with multilevel architecture	Installation of complex applications with multilevel architecture	Installation of complex applications with multilevel architecture	Installation of complex applications with multilevel architecture
Install patches and updates during the Middleware and Runtime lifecycle	Install patches and updates during the Middleware and Runtime lifecycle	Install patches and updates during the Middleware and Runtime lifecycle	Install patches and updates during the Middleware and Runtime lifecycle
Installation, additional software, libraries, executable environments: JAVA, .NET (Middleware and Runtime)	Installation, additional software, libraries, executable environments: JAVA, .NET (Middleware and Runtime)	Installation, additional software, libraries, executable environments: JAVA, .NET (Middleware and Runtime)	Installation, additional software, libraries, executable environments: JAVA, .NET (Middleware and Runtime)

Continuation of Table 1.1

Installation of patches and updates during the life cycle of the OS	Installation of patches and updates during the life cycle of the OS	Installation of patches and updates during the life cycle of the OS	Installation of patches and updates during the life cycle of the OS
OS installation and configuration	OS installation and configuration	OS installation and configuration	OS installation and configuration
Hypervisor installation and virtualization configuration (optional)	Hypervisor installation and virtualization configuration (optional)	Hypervisor installation and virtualization configuration (optional)	Hypervisor installation and virtualization configuration (optional)
Allocation of network resources (Physical ports, VLAN, IP addressing)	Allocation of network resources (Physical ports, VLAN, IP addressing)	Allocation of network resources (Physical ports, VLAN, IP addressing)	Allocation of network resources (Physical ports, VLAN, IP addressing)
Allocation of Storage System Resources	Allocation of Storage System Resources	Allocation of Storage System Resources	Allocation of Storage System Resources
Dedication of the physical server	Dedication of the physical server	Dedication of the physical server	Dedication of the physical server

The analysis showed that for the effective operation of the Internet of Things it is not necessary to send all IoT data to the "cloud", as it is much more expensive than processing them and including a border router in the area served by cloud service (Fog computing)

The work uses Fog computing technology to improve the IoT infrastructure and improve its performance. In cloud computing, a large amount of centralized storage and processing resources are available to distributed consumers through cloud network

structures for a relatively small number of users. In nebulous computing, a large number of individual intelligent objects communicate with nebulous network structures that perform computations and store resources near peripherals in the IoT.

Fog Computing solves problems caused by thousands or millions of "smart" devices, including security, privacy, limited network, and latency.

CONCLUSION TO CHAPTER 1

This chapter discusses the concept and aspects of the Internet of Things. I analyzed the architectures, core protocols, and technologies used on the Internet of Things. Examples of the pros and cons of the widespread introduction of the Internet of Things were given, and we saw scenarios for the application of technology in everyday life and production. In the long run, not only housing will become "smart", but also cities and even (some) states.

However, at this stage in the history of the Internet of Things, it is not actively implemented worldwide, but within companies engaged in the production of goods, energy, transport and other industries, where new technologies are expected to increase productivity and competitiveness. The problem of scaling this experience is related to the need to connect several systems from many suppliers into a single whole and develop their coordinated work.

Based on all the data reviewed and presented, it was concluded that the Internet of Things is already a very modern and useful technology, but so far there are a number of issues and problems that need to be addressed. We can identify problems with the speed of data processing and transmission, with the energy efficiency of IoT-based systems, as well as cybersecurity problems of such systems. Therefore, the purpose of this study is to consider the technology of computing’s and select the most useful of them to address these issues specifically, for which the following sections are selected Fog Computing.

CHAPTER 2
THE MAIN CONCEPTS OF FOG COMPUTING AND IT IS IMPLEMENTATION IN INTERNET OF THINGS

2.1. The concept and definition of the Cloud Computing

Cloud computing is becoming an important aspect of modern businesses' operations. However, in order to effectively use this technology, you must first grasp the cloud's basic characteristics, kinds, and what services may be employed to maximize cloud operations. A company's access to shared computer resources such as servers, storage, networking, apps, and other cloud services is known as cloud computing. The user may utilize and administer all resources without the need for extra help from the cloud service provider. Cloud Computing's Key Features. The following are the major aspects of cloud computing:

Requested self-service. You can do it yourself without the support of the provider's workers if you determine on Saturday night that you need to use the cloud's processing capacity as a network storage of information.

Internet Access for Free. To take use of cloud computing's benefits and services, you must first have network connectivity. Furthermore, you may access the services from a variety of devices, including a laptop or a mobile phone.

Resources consolidation. The service provider pools all cloud resources and makes them available to numerous leases. Your and other users' demands determine how virtual and real cloud resources are distributed. Storage, RAM, virtual machines, computational power, and bandwidth are examples of resources.

Fast scalability. The number of resources is promptly reserved and adjusted to your needs if necessary. Scripts are frequently used by providers so that you may purchase the resources you require at any time and in any number.

Resources are being pooled. All cloud resources are pooled together by the provider and made available to many leases. All virtual and real cloud resources are assigned based

on the demands of you and other users. Storage, RAM, virtual machines, processing power, and bandwidth are some of the resources available.

Scalability in a short amount of time If needed, resources are instantly reserved and scaled to meet your needs. Scripts are frequently used by providers so that you may purchase the resources you need at any time and in any number.

Service evaluation All resources are automatically monitored, measured, and adjusted to guarantee that you and the cloud provider operate with accurate data on the amount of services utilized. Computing power, the number of active users, storage space, bandwidth, and other resources are among them [10].

Models for Cloud Computing

Software as a Service (SaaS) is a type of cloud computing.

Using provider software that operates on a cloud infrastructure is what this cloud approach entails. Such software can be accessed via a client or program interface. It's critical to realize that if you utilize a SaaS service, you won't be able to handle cloud infrastructure like the operating system, network, storage, or server. Microsoft 365 is an excellent example.

Platform-as-a-Service (PaaS) - platform as a service.

You are given access to a cloud computing platform that includes all essential cloud languages, services, tools, and libraries from the cloud provider. You also have no control over the cloud infrastructure, servers, network, operating system, or storage. You can, however, control programs and some application environment configuration parameters. Microsoft Azure is an excellent example.

Infrastructure as a Service (IaaS) is a kind of cloud computing Infrastructure as a Service. You have enough computer power, storage, network, and other important computing resources to deploy and maintain whatever program you choose. Applications and operating systems are examples. You can't handle the cloud architecture, but you can adjust the operating system, installed apps, storage, and partially manage specific components like host firewalls. Google, IBM, Amazon, and other well-known service providers are among them [10].

2.2. Difference between Cloud and Fog Computing

Cloud computing is the process of using remote servers or computers over the Internet to perform data transfer, storage, and data management operations, rather than using a local computer or server. Cloud computing offers delivery services directly over the Internet. Cloud computing services can be of any type, such as data warehouses, databases, software, applications, networks, servers, and so on. Fog computing is a term coined by Cisco to mean extending services beyond cloud computing to enterprise needs. It consists of a decentralized computing environment in which the infrastructure provides storage, programs, data, and computing. Foggy computing is also called Fog Networking or Fogging. The main difference between nebulous computing and cloud computing is that the cloud is a centralized system, while fog is essentially a distributed decentralized infrastructure [12].

The main differences between cloud computing and fog computing

The cloud architecture has various components, such as storage, databases, servers, networks, and so on. While fog computing has all the features of cloud computing, including additional features of efficient and powerful storage and performance between systems and cloud networks. The cloud computing architecture system can be divided into two sections, such as front and rear, in which both will be connected in a network, while fog computing extends cloud computing by providing functions at the network boundary.

The front end of cloud computing is called the user interface, where end users or customers use cloud computing services, where the back end is the cloud part of the cloud computing network, while fog computing is intended to improve efficiency and reduce data transformation or data transfer and transfer operations. distributed in different places.

The client can access different types of services through the front section of cloud computing, where the user can access services, usually as a local computer, but which can be accessed by connecting to a network, while fog computing is supported by a large consortium of an open group called the Consorum Open Fog, which was formed in November 2015 by a group of companies such as Cisco, Dell, Microsoft, Intel, ARM and Princeton University.

In cloud computing, the back section is servers, different computers, storage systems, and databases interconnected to form a cloud network distributed in different locations, while Fog computing processes data on a central server, collecting data from different devices that are deployed over long distances or in different places, away from the central server.In cloud computing, more memory space is required for clients to access their stored data, almost memory space will be available twice as much data is stored to provide high-speed access, while fog calculates data operations and calculations are performed in the central hub of the device to reduce the conversion of data from and to the central server [12].

In cloud computing, there is a central server for administering or managing different computers or servers connected to each other, their interaction and mechanisms will be monitored and controlled, while fog computing supports most IoT devices - Internet of Things compared to cloud computing, ensuring greater compliance and ease of migration.

Next to the central server, there is intermediate software for establishing a protocol between multiple servers and secure and secure communication with each other, while Fog Computing supports many IoT and big data applications, processing large amounts of data and different devices.

All data stored in the central repository of the database server will be available as a backup to make it highly available in case of a few server failures, which is called redundancy, while Fog Computing has a greater distribution in geographical areas due to the support of a large number of users online effectively [12].

The main component of cloud computing is the Internet / network, without which the whole network collapses and there is no possibility to connect to cloud servers, while Fog Computing has a variety of programs, from the Internet of Things to human-machine interaction, from broad programs.

A large number of end users can connect to cloud servers from remote machines using virtual device interfaces called virtual machines, in which the concept is called virtualization, while fog calculations can be considered each time large amounts of data are collected in extreme cases such as edges. railways, ships, vehicles and roads, etc.

Table 2.1

Difference between cloud and fog computing

	Cloud computing	Fog computing
Delay	Cloud computing has low latency, but not compared to fog	Foggy computations have low latency in terms of network
Capacity	Cloud computing does not reduce data when sending or converting data	Fog Computing reduces the amount of data sent to cloud computing.
Throughput	Cloud computing saves less than Fog Computing	Fog Computing stores the amount of throughput.
Sensitiveness	In cloud computing mode, the system response time is low.	For fog calculations, the response time of the system is large.
Security	High, but smaller compared to foggy calculations	High security
Speed	Access speed is high, depending on the VM connection	High even more compared to cloud computing
Data integration	You can integrate multiple data sources	You can integrate multiple data sources and devices

2.3. Technical aspects of implementation in Internet of Things and differs from Edge Computing

The Internet of Things (IoT) is the networked integration of any devices (things) to enhance their usefulness. The finest example is a "smart house" system that can maintain a pleasant temperature, humidity, and other environmental parameters on its own. Special sensors monitor current performance, and the system subsequently switches on the air conditioner, thermostat, humidifier, or other equipment based on your preferences [13].

Fog and Cloud Computing Layers

Big data that are generated by different IoT applications presents a new characteristic called Geo-distribution. This new dimension requires that the sensed information has to be processed at the edge of the network area close to the smart devices instead of processing it by remote servers of cloud computing. It is worth mentioning that it is indispensable to offer low latency response in order to allow smart objects to take the right action at the suitable time and to protect the integrity of sensitive infrastructure components. As a result, fog computing paradigm was suggested to extend cloud-computing services to the edge of IoT networks, to provide a highly virtualized platform that supplies many networking, storage and computational services between smart devices and cloud computing services. Fog architecture comprises of four layers as depicted in Figure 2.1., which are monitoring, pre-processing, storage, and security layers [13].

Fog Layers Architecture

1. Monitoring layer: This layer is responsible for observing the activities of smart devices and networks. For example, it detects which sensor node performs some tasks, what task the node performs and at what time it is executed. Besides, this layer is in charge of monitoring the energy level of different network devices.

2. Pre-Processing layer: Performs data management, analyzing, filtering and trimming processes to generate useful and meaningful data.

3. Temporary storage layer: After the pre-processing layer processes sensed data, it will be stored temporarily in the resources of this layer. The temporary storage layer offers many storage functionalities such as data storing, distribution, and replication.

4. Security layer: It implements encryption and decryption techniques to protect the privacy and integrity of data.

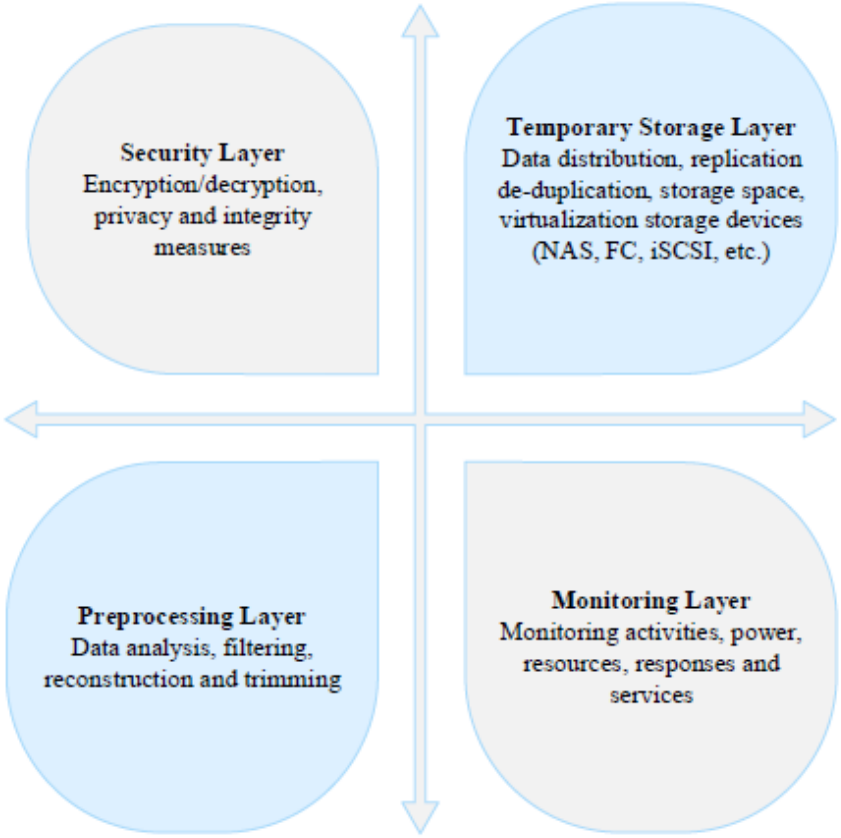

Fig. 2.1. Layered architecture of fog computing [13]

Why to Use Fog Computing Nodes

Fog computing nodes act as a bridge between smart objects, storage services, and large-scale cloud computing servers. This model extends network resources and services to the underlying network, so it has the capability of providing end-users with better delay performance services. Despite that, there is an important difference between the cloud and fog computing paradigms, where the cloud has enormous computational, communication and storage capabilities compared with fog computing, Figure 2.2. shows the roles of cloud computing and fog computing in the delivery of IoT services [13].

Connecting a massive number of smart objects to the internet such as smartphones, PCs, animals, and humans tracking, creates what is called the “Big Data” term that needs high capabilities to be stored, processed and analyzed. Fog computing nodes provide end-users with such abilities and are the best choice for many applications rather than farthest cloud computing for the following reasons:

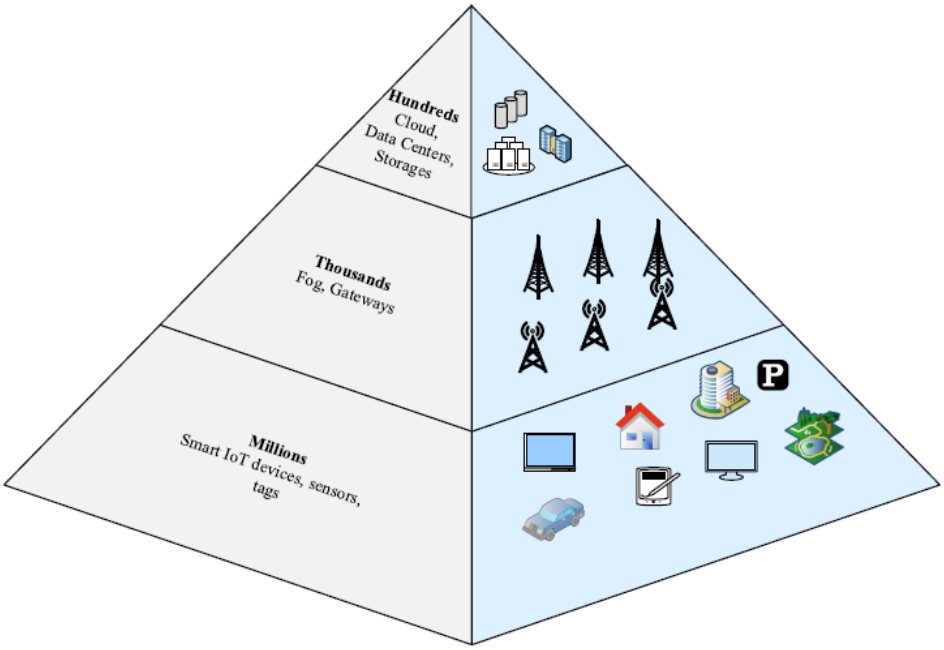

Fig. 2.2. Roles of Cloud and Fog Computing in the delivery of IoT services [14]

1. Edge location, low latency, location awareness: According to that, fog computing provides its clients with rich applications and services with low latency requirements.

2. Geographical distribution: Applications and services that are hosted and processed by the fog nodes require widely distributed deployment of these nodes closer to the end-user. Fog, for instance, plays an essential role in delivering quality streaming to vehicles via access points and proxies that are positioned along tracks and highways.

3. Mobility supporting: It is common that fog applications communicate directly with mobile smart entities. Thus, fog computing is able to support mobility standards such as locator identifier separation protocol.

4. Real-time interactions: It has the ability to implement real-time interaction services since it can give an instantaneous response.

5. Dominance of wireless access.

6. Supporting online analytic and interaction with the cloud, as it plays a significant role in the ingestion and processing of a massive amount of data that are received from close smart devices.

7. Scalability: Fog permits IoT environments to grow, so as the number of smart devices increased, as a result, the number of fog nodes will be increased too to handle the

new load. Such resource expansion cannot be achieved from the cloud side since the deployment of new servers is highly cost.

8. On the fly analysis: Fog resources aggregate data to transmit it partially processed to the cloud servers for additional processing.

9. Power constraints: Since most of the smart devices are battery-powered, long-distance communication toward the cloud will deplete their energy faster [14].

Cloud computing architecture

In the IoT model, communication and information systems are embedded in the intelligent environment around us. This will produce a huge amount of data that needs to be presented, processed and stored in an efficient, seamless and easy to understand way. According to, cloud computing is the latest paradigm to demonstrate its efficiency, scalability, autonomy and reliability, providing high opportunities for the study of dynamic resources, ubiquitous access and composition6 that are important for future prosperity. IoT applications [14]. This platform performs a number of roles, such as a data receiver for smart devices, a computer that analyzes and interprets different types of data, and a web visualization provider. Many researchers are trying to build a compatible architecture that could describe the function of the cloud computing paradigm, as shown in Figure 2.3. This model consists of three layers, namely, the base layer, which contains a database for storing data for all smart devices on the IoT. The next level is the component level that contains the code needed to interact with all IoT objects, and uses a subset of these objects to perform a service or request their status, where the last level in this model is the application level that corresponds to in order to provide users with the necessary services [14].

Cloud and Fog Based Architectures

Let us now discuss two kinds of systems architectures: cloud and fog computing (see the reference architectures in).

In particular, we have been slightly vague about the nature of data generated by IoT devices, and the nature of data processing. In some system architectures the data processing is done in a large centralized fashion by cloud computers. Such a cloud centric architecture keeps the cloud at the center, applications above it, and the network of smart things below it. Cloud computing is given primacy because it provides great flexibility and scalability. It

offers services such as the core infrastructure, platform, software, and storage. Developers can provide their storage tools, software tools, data mining, and machine learning tools, and visualization tools through the cloud [5].

Lately, there is a move towards another system architecture, namely, fog computing, where the sensors and network gateways do a part of the data processing and analytics. A fog architecture presents a layered approach as shown in Figure 2, which inserts monitoring, preprocessing, storage, and security layers between the physical and transport layers. The monitoring layer monitors power, resources, responses, and services. The preprocessing layer performs filtering, processing, and analytics of sensor data. The temporary storage layer provides storage functionalities such as data replication, distribution, and storage. Finally, the security layer performs encryption/decryption and ensures data integrity and privacy. Monitoring and preprocessing are done on the edge of the network before sending data to the cloud.

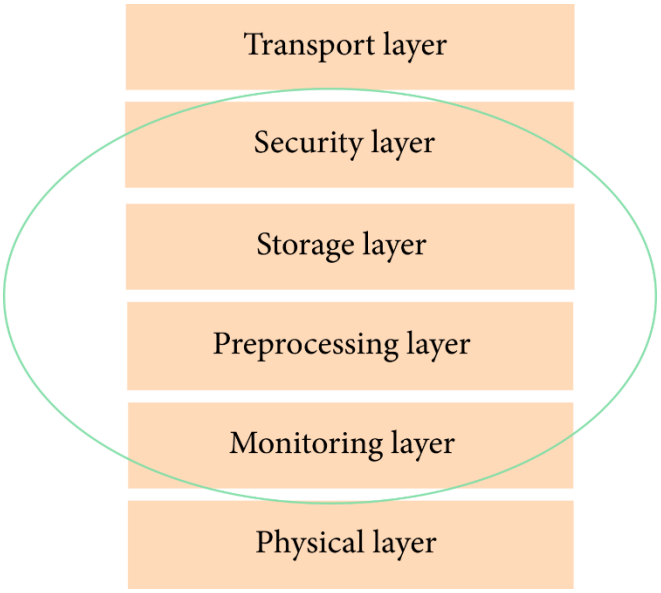

Fig. 2.3. Layers of Fog and Cloud Computing in Internet of things [5]

Fog architecture of a smart IoT gateway.

Often the terms “fog computing” and “edge computing” are used interchangeably. The latter term predates the former and is construed to be more generic. Fog computing originally termed by Cisco refers to smart gateways and smart sensors,

whereas edge computing is slightly more penetrative in nature [5]. This paradigm envisions adding smart data preprocessing capabilities to physical devices such as motors, pumps, or lights. The aim is to do as much of preprocessing of data as possible in these devices, which are termed to be at the edge of the network. In terms of the system architecture, the architectural diagram is not appreciably different from Figure 2.3. As a result, we do not describe edge computing separately.

Finally, the distinction between protocol architectures and system architectures is not very crisp. Often the protocols and the system are codesigned. We shall use the generic 5-layer IoT protocol stack (architectural diagram presented in Figure 2.3.) for both the fog and cloud architectures [5].

The main differences between edge computing and fog computing

Peripheral computing is an approach that involves processing data at the edge of the network where the data is created, rather than in a centralized repository designed to process data. Border computing systems are a distributed open IT architecture that uses decentralized processing and provides support for mobile Internet of Things technologies. When using peripheral computing, the data is processed by the device itself, the local computer or the server, and not transferred to the data center [15].

Boundary computing systems provide acceleration of data flows, including real-time data processing without delay. They allow intelligent programs and devices to respond to data almost immediately after their creation, eliminating any delays. This is critical to the development of technologies such as autopilot vehicles, and provides important benefits for organizations

Boundary computing provides efficient processing of large amounts of data near the source, reducing the load of Internet channels. On the one hand, this reduces costs, and on the other - to effectively use programs remotely. In addition, the ability to process data without placing it in the public cloud provides an additional level of protection for sensitive data [15].

In turn, nebulous calculations always use boundary calculations, but not vice versa. Fogging is a system-level architecture that provides tools for distributing, organizing,

managing, and providing resources and services across networks and between peripheral devices.

Boundary computing architectures host servers, applications, or small clouds on the periphery. Fog computing has a hierarchical and flat architecture with multiple layers forming a network, while boundary computing relies on individual nodes that do not form a network.

Fog computing has a wide range of peer-to-peer relationships, where each boundary performs its nodes in silos (network fragments isolated from each other), which requires cloud data transfer for peer-to-peer traffic. It is also worth noting that foggy calculations include the use of cloud services, while boundary calculations exclude the use of food in general [16].

Table 2.2

Differences between Edge and Fog Computing

Edge Computing	Fog Computing
When compared to fog computing, it is	When compared to edge computing, it is extremely scalable
There are billions of nodes	There are millions of nodes
The nodes are placed distant from the cloud	The computer nodes in this system are located closer to the cloud (remote database where data is stored)
Fog computing is subdivided into edge computing	Fog computing is subdivided into edge computing
The amount of bandwidth required is little. Because the data is generated by the edge nodes themselves	The amount of bandwidth required is considerable. The data generated by edge nodes is sent to the cloud
The expense of doing business is greater	Operational costs are cheaper in comparison

Continuation of Table 2.2

High levels of privacy. Data breaches are extremely rare	Data breaches are more likely to occur
The incorporation of IoT devices or the client's network is known as edge devices	Fog is a cloud layer that has been expanded
Nodes have a low power consumption.	The power consumption of nodes filters vital data from the vast volume of data acquired from the device and keeps it in a high-performance filter.
Edge computing enables devices to get quicker outcomes by processing data received from several sources at the same time.	By delivering the filtered data to the cloud, fog computing assists in filtering critical information from the enormous quantity of data acquired by the device.

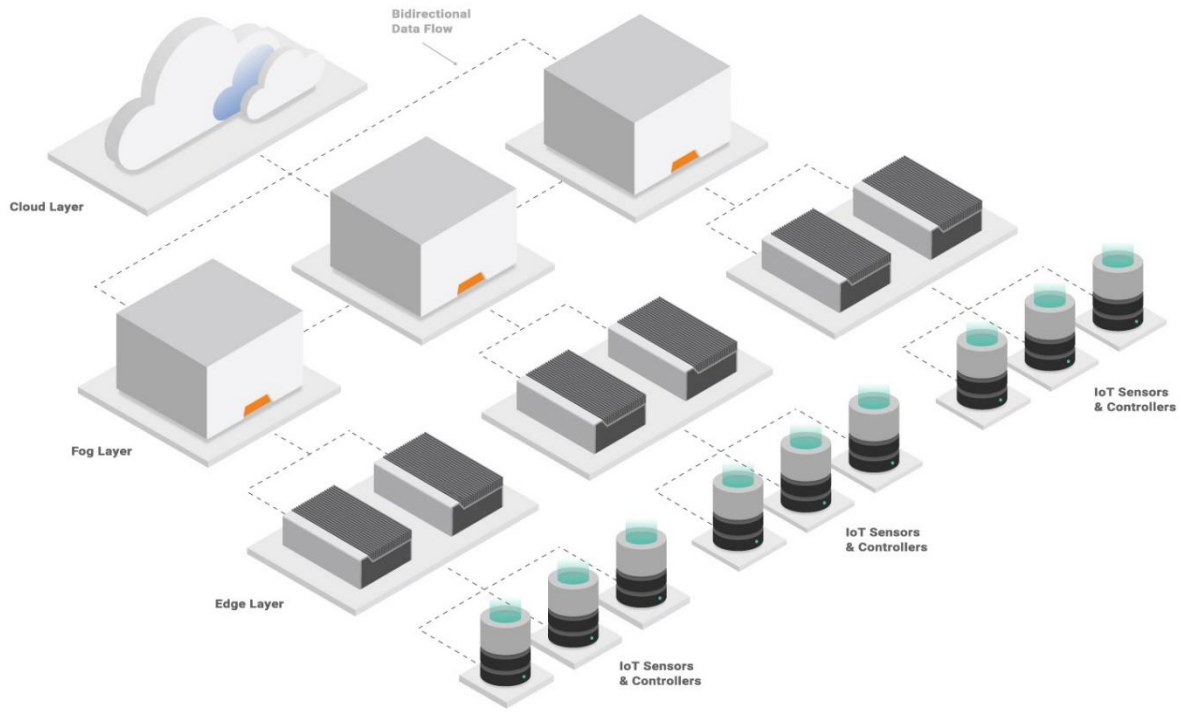

Fig.2.4. Example architecture of IoT/edge/fog/cloud computing system [16].

2.4. Role of "cloud" and "fog" in Internet of Things

The Internet of Things connects billions of devices to the Internet, with the majority of these devices having limited resources. In order to overcome the limitations of these tools and achieve the scope's needs, an intermediate computing level is required. Fog calculation is the most recent offspring of functional unit separation on a physical level. It is a computer layer that brings computing, network, and storage capabilities closer to the detection level, where sensors and actuators are placed. The Tooth layer provides the functionalities listed below to provide various IoT services and criteria [17].

Fog Computing is a highly virtualized platform that connects end devices to traditional Cloud Computing Data Centers, which are often but not always positioned at the network's edge, to provide computing, storage, and networking services. Figure 2.4 depicts a hypothetical information and computing architecture for future IoT applications, as well as the role of fog computing. Both the Cloud and the Fog are made up of compute, storage, and networking resources. "Edge of the Network," on the other hand, implies a variety of properties that distinguish the Fog as a non-trivial Cloud extension. Low latency, edge location, and location awareness. The Fog's beginnings may be traced back to early ideas to serve endpoints with rich services at the network's edge, including applications that demand low latency (e.g. gaming, video streaming, augmented reality) [18].

Geographical distribution is important. Unlike centralized clouds, Fog's services and programs necessitate a large-scale deployment. Fog, for example, will play a key part in delivering high-quality streaming for cars traveling over roads and rails via proxies and access points. Distributed systems that need distributed processing and storage resources include large-scale sensor networks for environmental monitoring and the Smart Grid [18].

Because of the large geographical spread, there are a lot of nodes, as proven by sensor networks in general and Smart Grid in particular. Distributed systems that need distributed processing and storage resources include large-scale sensor networks for environmental monitoring and the Smart Grid [18].

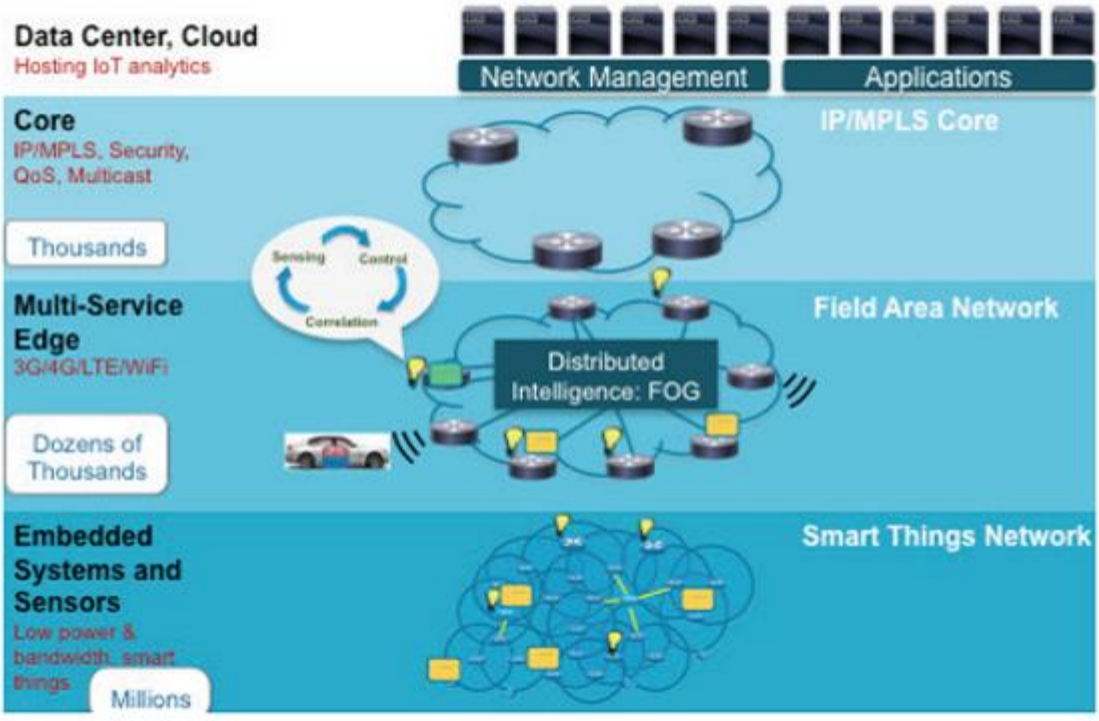

Fig.2.5. Connection of Fog Computing and Internet of things [13].

Because of the large geographical spread, there are a lot of nodes, as proven by sensor networks in general and Smart Grid in particular.

Assistance with mobility. Many Fog applications require a distributed directory system to connect directly to mobile devices, therefore they enable mobility approaches like LISP 1, which separates the host ID from the location ID.

Interaction in real time. Real-time interaction, rather than batch processing, is required for important fog projects. The domination of wireless connectivity.

Heterogeneity. Fog nodes come in a range of forms and are used in a number of settings.

Compatibility and cooperation. Full support for some services (streaming is a good example) necessitates collaboration between multiple service providers. As a result, Fog components must communicate with one another and services must be consistent across domains.

Supports cloud-based online analysis and collaboration. Near the source, the Nebula has been discovered to play a crucial role in data collecting and processing [18].

Table 2.3

Relationship between the parameters of the Internet of Things and Fog/Cloud Computing

Parameter	Internet of Things	Fog and Cloud computing
Data arrays	Acts as a source of data arrays	Acts as a way or means to manage data arrays
Data reachability	Very limited	Long range
Data warehouse	Limited or almost non-existent	Great, almost never ending
The role of the Internet	Acts as points of convergence	Acts as a means of providing services
Computing capabilities	Limited	Virtually unlimited
Components	Runs on hardware components	Runs on virtual machines that mimic hardware components

2.5. Practical application of "fog" in the Internet of Things

System for Autonomous Vehicles (ADS). ADS employs a number of multi-mode sensors, computer vision and image processing technologies, satellite and network placement on maps, and Intelligent Analytics to assist a driver or self-propelled vehicle in driving. Due of the high speed required for such applications, a fog-node with artificial intelligence features must be installed directly in the vehicle.

eHealth fog systems In medicine, fog systems are employed when it is required to swiftly assess data acquired from the patient's sensors and respond in line with the treatment plan [19].

Fog technology is now being utilized to monitor the state of diabetic patients and administer automated injections in specific circumstances.

The sensor on the patient's body identifies the crucial blood sugar level and sends a signal to a micro syringe, which is also on the patient's body, to administer the injection. As a result, the patient is relieved of the necessity to make measurements and injections on a regular basis.

Cloud provider ventures in the fog. In 2016, Amazon, Google, and Microsoft, the three main cloud platform providers, started various initiatives to deploy Fog Computing in their IoT ecosystems, which use the so-called "serverless architecture."

The server-free design enables you to run the source code of hundreds or millions of users (including fog devices) without having to worry about resource scalability [19].

Microsoft has announced that the Software Development Kit will support Azure Functions (SDK).

Azure features were first released as part of Microsoft's Serverless Architecture cloud product line.

When dealing with the AWS cloud platform, Amazon has built the Greengrass platform to facilitate so-called Lambda-functions (server-free architecture) in IoT devices. Greengrass is a software module execution container that runs directly on a Fog device rather than a data center server. Greengrass-enabled devices may communicate with one another regardless of external Internet access, i.e., horizontally amongst Fog devices utilizing different Internet of Things radio protocols.

Google has announced the Android Things Internet platform, which will support Intel Edison and Joule 570x microcomputers, as well as NXP Pico i.MX6UL and Argon i.MX6UL and Raspberry Pi 3. Fog apps are created for any of these devices using the Android Studio platform. Android Things also works with Google Play and the rest of the Android ecosystem, which currently powers 90% of all smartphones on the planet. As a result, any Android smartphone or tablet may act as a Fog node thanks to the Android Things system [19].

In the next part we will consider the practical application of Cloud Computing in the Internet of Things, for which we will build and analyze the IoT platform based on Cloud Native technology.

CONCLUSION TO CHAPTER 2

Cloud computing is a technology that allows you to provide computer power on demand, as well as store databases, applications, and other IT resources. It enables enterprises to use computer resources such as a virtual machine (VM) rather than constructing their own computing infrastructure. Many companies, including Amazon, Alibaba, Google, and Oracle, are developing machine learning tools that use cloud technology to provide a variety of solutions to organizations all over the world.

After reviewing and analyzing the Internet of Things, the question arose of improving its weaknesses, namely the speed of calculations and data transmission, information security and energy efficiency. Among the types of calculations reviewed in this section based on the data shown for the intermediate stage between devices and the "cloud" was chosen Fog Calculations that allow you to use the resources of the device to transfer to the cloud pre-processed data.

As the Internet of Things has grown, it has become clear that data must be filtered and pre-processed before being sent to the cloud. The following are the programs in general:

Gaming applications and video conferencing are examples of applications that demand a short and predictable latency in data transfer across the network.

Unmanned vehicles, high-speed trains, intelligent transportation systems, and other transportation applications

Intelligent power supply systems (Smart Grid), intelligent transportation systems (ITS), geophysical exploration, pipeline management, sensor networks for environmental monitoring, and other applications that need local real-time data processing

Fog is not a replacement for Cloud. Fog, on the other hand, works well with the Cloud, particularly in data management and analytics, and this relationship gives rise to a new class of applications.

CHAPTER 3
IOT NETWORK ARCHITECTURES WITH LORAWAN PROTOCOL

3.1. Theoretical part

IoT device energy consumption is a major concern, particularly for large-scale application of these technologies in the near future. A substantial quantity of energy is required to link billions of devices to the Internet.

The issue of energy economy in IoT systems necessitates proper communication protocol selection during system design. There is a difficulty with replacing power supply in IoT devices if you respond incorrectly. Replacing power sources on a regular basis raises the expense of sustaining such a system, making it unprofitable to operate [20].

You may choose between three protocols to reduce energy consumption: Sigfox, LoRaWAN, and NB-IoT. The terminals in Sigfox, LoRa, and NB-IoT are primarily in sleep mode, which minimizes energy consumption and hence terminal durability. However, because of synchronous communication and QoS processing, the NB-IoT terminal uses more power, and OFDM / FDMA access modes demand a higher peak current. In comparison to Sigfox and LoRaWAN, this extra power consumption affects the life of the NB-IoT terminal. NB-IoT, on the other hand, has the advantage of low latency. Unlike Sigfox, LoRaWAN uses Class C to handle minimal bidirectional latency while using more power. As a result, Sigfox and LoRaWAN Class A are the ideal options for applications that aren't sensitive to delays and don't deliver a lot of data. NB-IoT and LoRa Class C are the best options for low-latency applications. Based on the conditions described above, the LoRaWAN protocol was chosen for our work [20].

Standard architecture of LoRaWAN protocol.

Because of the openness of the LoRaWAN protocol, you may create and operate private LoRaWAN networks in which the owner can change some aspects of the network design. The standard elements of the LoRaWAN network are summarized in the following list.

Terminals - sensors or actuators that can communicate wirelessly with gateways utilizing the LoRa radio frequency modulation standard. The terminals are typically powered by batteries.

Gateway - Acts as a bridge between a LoRaWAN and an IP network, such as Ethernet or Wi-Fi. The gateway acts as a terminal's input signal to the LoRaWAN network, converting RF signals into IP packets and forwarding them to the appropriate network server.

Network server - the network's central hub that controls and administers the network. The network server controls adaptive data rate schemes and filters duplicate or superfluous packets, among other things. Sends packets from end devices to the application server that is connected with them.

Application Server - handles all application layers' payload. The data is then used by the application server to conduct tasks including decrypting, saving, and presenting the database over a web user interface. Gateways are the nearest portion of the network to the endpoint in the conventional LoRaWAN network architecture depicted in Fig. 3.6. Because it does not undertake computing activities, each gateway operates as a passive region in the network [21].

The gateway accepts data from the endpoints and turns it into packets that may be transported and processed further. The transformed data is subsequently transferred to a network server that is connected. Data processing, computation, and storage are all handled by the application server. The LoRaWAN computing model is shown to conform to the cloud computing paradigm in the description.

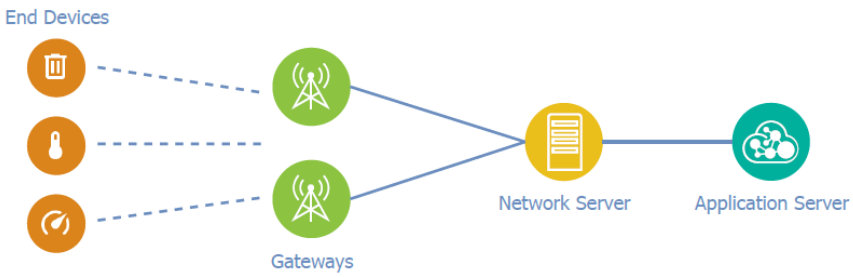

Fig. 3.6. LoRaWAN typical architecture [21]

Architectures of Network

The following is the study's primary point. If the fundamental pieces of LoRaWAN are modified, they may be changed into an architecture that supports the nebulous computing paradigm. The encryption of the program payload between endpoints, which is encrypted between the end device and the application server, is the key issue. As a result, the gateway is unable to access the encrypted data, preventing it from being processed and stored. Two session keys are kept in the end device's memory:

• NwkSKey (Network Session Key) - The network server and terminal utilize this key to analyze and validate the message integrity code (MIC). Data integrity in data messages is ensured by MIC. It is saved on the terminal and network server after successful activation [22].

• AppSKey (Application Session Key) - This key is used to decrypt and encrypt the payload of the application. It is saved on the end device and the application server after successful activation. Because the program's payload isn't complete, there's a chance the network server will alter the data message's content. Network servers, on the other hand, are often regarded as dependable. Each end device has its own set of partition keys. Three distinct network architecture concepts are described in the following paragraphs. After that, we compare these ideas to see which one is best for queuing theory.

Architecture 1

The architecture 1 that has been proposed is built on the concept of combining all standard parts of the LoRaWAN network into a single device known as a fog gateway. As a result, each gateway functions as a private network and application server in addition to receiving, converting, and forwarding packets. Based on current statistics, this modification may result in a speedier response. Fogging, on the other hand, isn't always essential or even practical. Given the limited processing capacity of nebulous transitions, transmitting particularly large volumes of data can be disproportionately onerous. This approach solves the problem by adding a distant cloud application server to the mix of fogged gateways. For all fogged gateways, only one cloud server is accessible for the whole LoRaWAN network [22]. For controlling gateways, devices, and applications, this cloud server provides a web interface and API. In Figure 3.7., you can see a schematic of architecture 1.

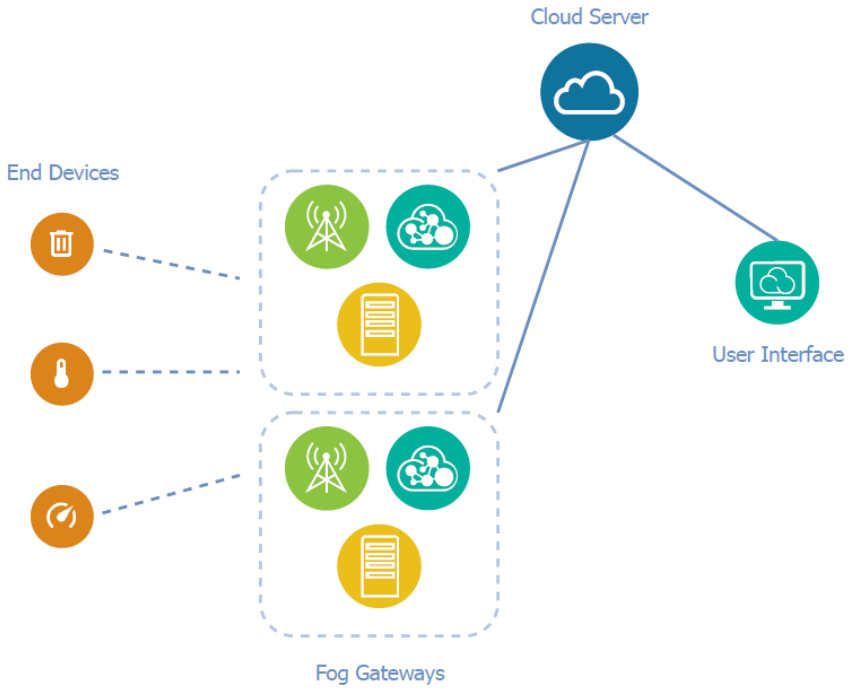

Fig. 3.7. network of architecture 1 [21]

Architecture 2

The approach to optimization in Architecture 2 is a little different. Unlike architecture 1, the proposed architecture 2 does not require network and application servers to be integrated in each gateway, instead requiring only one gateway in the network. Other gateways in the network can only receive, convert, and forward packets and perform the same functions as gateways in a typical LoRaWAN network. The correct operation of such a proposed architecture necessitates the use of a certain communication paradigm. Because one complicated node controls numerous nodes with minimal logic, the master-slave model is used. A master is a communication architecture in which one master controls and mediates communication among several subordinate nodes. These master and slave nodes are gateways in this scenario. The slave gateways use the standard LoRaWAN gateway method of operation. The slave gateway passes all received messages to the master gateway in this mode. To decrypt the payload and regulate packet forwarding by slave nodes, the primary gateway incorporates network servers and application servers. Due to restricted processing and fog gateway storage capabilities, the architecture includes a distant cloud server [23]. The cloud server uses the Internet to connect to the main gateway and store long-term data.

Fig. 3.8. depicts Architecture 2. The key benefit of this architecture is that each gateway does not need to be connected to the Internet. Because the network and application servers are hosted in the cloud, using the conventional LoRaWAN architecture necessitates an Internet connection. Because it talks with a distant cloud server, only the gateway in Architecture 2 can connect to the Internet.

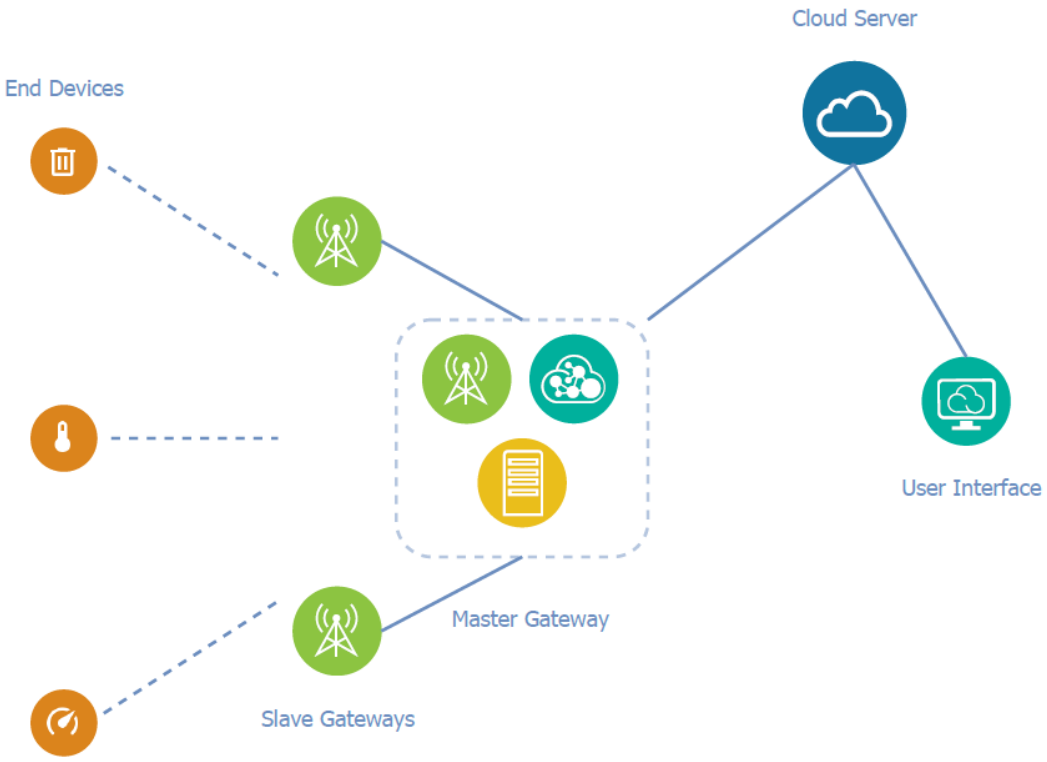

Fig. 3.8. network of architecture 2 [21]

Architecture 3

Unlike earlier architectural improvements, Architecture 3 follows an entirely new philosophy. The key difference here is the link between the gateway and the application server, rather than regrouping certain pieces of the normal LoRaWAN architecture. As a result, Design 3 is identical to the conventional LoRaWAN architecture [23]. Because end-to-end encryption prevents the LoRa gateway from knowing the session keys, it is unable to access the encrypted payload because decryption is handled by the application server. The primary idea behind optimization is to negotiate between a specific gateway and the application server in order to get and then store the keys required for each end device in a

locally secured database. This enables the gateway to connect with the application server only when it lacks the requisite session keys for a specific endpoint or when it is required. This reduces the amount of time spent interacting with the application server. The network operator may add a nebulous gateway to an existing LoRaWAN network without modifying the cloud layer, which is a substantial benefit of architectural design. A schematic of the architecture is shown in Fig. 3.9.

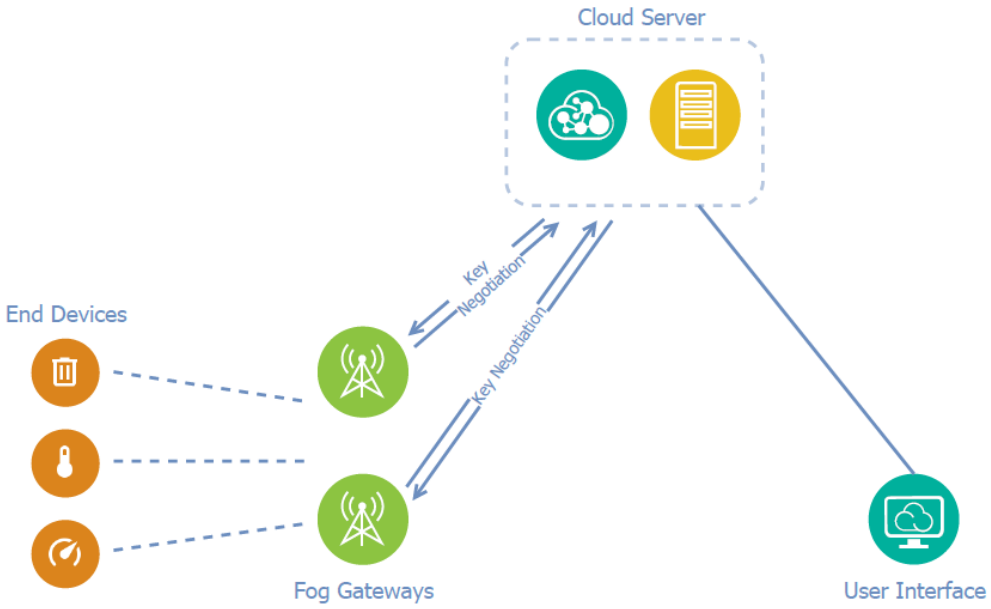

Fig. 3.9. Network of architecture 3 [21]

6. Comparison of service times

Because the Internet of Things network may be thought of as a queueing system, the idea of waiting can be applied to compare the suggested designs in terms of service time. Service requests can be regarded individual communications from end devices. Queues for the LoRa gateway, network server, and application server. The gateway queue node includes eight servers that can handle requests concurrently, assuming the gateway can receive up to eight LoRa messages simultaneously with different SFs on various channels [24]. To ensure that all of the suggested designs have the same criteria, all terminals are assumed to be of class A, employ the ABP activation technique, and deliver messages without confirmation. Because all architectures consider the same physical layer (LoRa), modeling focuses on the

data processing done by each part of the architecture. Simulating the behavior of a single terminal during messaging is required for accurate data processing simulation. IoT devices, such as sensors, trackers, and other similar devices, frequently communicate their data at predetermined intervals. A superposition of deterministic point processes may be used to describe the entire traffic from a large number of these IoT devices. This procedure may be described using the Poisson process if these discrete point processes are deemed independent and each device generates its signals independently of the others. Arrival time, which is the time between terminal messages in terms of the LoRa gateway, may be used to represent aggregate traffic. The error element is incorporated in the Poisson approximation while transmitting a message for particular end devices due to the presence of this periodicity. Messages and their payloads, on the other hand, fluctuate in size depending on the IoT network's actual environment. As a result, the length of service is governed by the variable and exponential distribution [24].

3.2. Practical part

To calculate the runtime for each constituent of each design, a set of experimental measurements were carried out. A Raspberry Pi 4 Model B with 2 GB of RAM and the Raspbian operating system were utilized in the LoRa gateway hardware. A virtual machine with 2 GB of RAM and the Debian operating system is chosen, providing enough computational capacity to handle network and application server responsibilities. Because the time of message propagation in the radio environment was not significant for these experimental measurements, execution time was measured from the time the message was received by the gateway. The findings were calculated with a 95% confidence level. The execution time of the gateway (packet forwarder) (T_{pktfwd}) was measured for the proposed architectures 1 and 2 until the message was passed to the network server, which continued to process the message. The network server's execution time was calculated from the time the message was received to the time the message was processed and transmitted to the application server. The application server's runtime was calculated from the time the message was received until the encrypted payload was uploaded to the database [25]. A

total of 1000 mails were used in the experiment. The average time was then determined. The results of these experimental measures are shown in Table 3.3.

Table 3.3

Execution times of the components

Component	Average Execution Time (ms)
Packet forwarder (gateway)	0.15
Network Server	193.68
Application Server	14.17

Because the packet forwarder in Architecture 3 has been particularly adapted to execute fog calculating tasks, it employs a different technique. The packet forwarder in this situation is intended to forward data to a network server as well as decode messages and payloads. As a result, the packetforwarder must include the execution time of each fog calculation function performed by the gateway, such as decoding the message (Tdecode), decryption of usable data (Tdecrypt), and subsequent storage of useful data in the database (Tdatabase).

$$Tfog = Tdecode + Tdecrypt + Tdatabase\ , \tag{3.1}$$

$$Ttotal = Tpktfwd + Tfog, \tag{3.2}$$

The aforementioned equations may be utilized to calculate the overall message execution time necessary to conduct the fog calculation functions associated with the proposed architecture 3 using the above formulae. The Raspberry Pi 4 Model B was employed as a gateway for experimental measurements, same like in the prior scenario. Thousands of measurements of the many functionalities were carried out throughout time. To measure each decoding and decryption operation, the program created a pseudo-random string of at least 20 characters. To get the final time component, we monitored metadata storage and payload in the database [25].

The complete findings of the experimental measures are shown in Table 3.4.

Table 3.4

Experimental measurement findings descriptive statistics (miliseconds).

Time	A	B	Min.	Max.	Mid.	C	D	E	F
T_{decode}	1.93	0.91	0.85	5.04	1.68	1.55	1.93	2.32	6.89
$T_{decrypt}$	1.20	1.44	0.18	5.79	0.55	0.46	1.16	2.25	6.67
$T_{database}$	7.03	2.97	1.04	24.25	5.83	5.62	6.47	2.45	9.56

Table 3.5 shows the average total time required by the gateway to process messages. These times were determined from the above equations.

Table 3.5

Execution times of the fog gateway.

Time Component	Execution Time (ms)
T_{fog}	10.21
T_{total}	10.37

In question of increasing performance, using Fog Computing, vendors and developers a lot of different platform (Nuclio, for example), most of them handles around 400,000+ functions per second, is the best choice, as the Knative platform, for example, handles around 256,000 functions per second. Therefore, by choosing the Nuclio platform, we get better computing data transfer speeds. For Cloud Computing, this parameter is 360,000 functions per second, which means that the selected technology increases performance by an average of 10%.

IoT security and privacy risks are increasing along with the benefits of embracing IoT technologies. This is largely due to the fact that the Internet of Things links billions of devices to the Internet and requires the protection of billions of data points. Attackers obtain access to the network by utilizing IP devices that aren't well-protected. Because IP devices are so tightly linked, a hacker only has to exploit one vulnerability to corrupt all of the data

and render it useless. As a result, manufacturers that do not update their gadgets on a regular basis - or at all - leave them open to hackers. Users of connected devices are frequently asked to provide personal information such as names, ages, addresses, phone numbers, and even social network accounts, all of which are useful to hackers. Hackers aren't the only ones that pose a threat to the Internet of Things. Another key concern for IP users is confidentiality. Companies that develop and distribute consumer products, for example, may utilize those devices to collect and sell personal information from consumers [26].

Cloud computing is one of the most effective computing paradigms for IoT data processing. More efficient ways are needed to delay and limit the bandwidth of centralized data processing resources. Foggy computing is a cloud extension and distributed architecture that brings computing and analytics services closer to the network. Foggy computing is a cloud computing concept that scales up the cloud to serve greater workloads. In nebulous computing, a nebulous node is any device that can compute, store, and connect to a network. Personal computers, industrial controls, switches, routers, and embedded servers are just a few examples of these devices. Instead of transmitting IoT data to the cloud, fog processes and stores it locally on IoT devices under this computing paradigm. Improved secure services, which are necessary for many IoT applications, as well as decreased network traffic and latency, are among the advantages of this strategy. As a result, unlike cloud computing, fog provides processing and computing capabilities that are more responsive and secure. This enables you to make judgments and take relevant action more quickly [26].

Foggy computing is the flow of data between a conventional cloud, data centers, and Internet of Things devices or services, such as storage, in a dispersed environment. Cisco created the term "closed extension of things to the IoT data cloud," which may be described as a closed extension of things to the IoT data cloud. Many ubiquitous stand-alone technologies collaborate in a decentralized setting in the fog computation scenario. These gadgets work independently to process and store data. Cloud data centers are used in fog computing to offer services to IoT infrastructure. High mobility, computing resources, communication protocols, and diverse infrastructure interfaces are all supported by fog computing. Fog computing is a decentralized computing architecture in which data is

processed and stored in the cloud infrastructure between the source and the cloud infrastructure. This reduces the need to process and store huge volumes of duplicated data by lowering the extra cost of data transport and improving processing performance on a typical cloud platform [27].

Data processing at the network boundary is one of the primary elements of nebulous computing, which is why it's also known as boundary computing. Low latency and real-time interaction between user terminals and fog nodes are possible because processing resources are accessible at the network boundary. Only the essential portion of useful data is sent to the cloud, and superfluous data is not sent over the Internet, reducing bandwidth consumption. A platform of static and mobile computing resources is supported by fog nodes. Another characteristic of nebulous computations is that they must be diverse. Fog assemblies and terminals are manufactured by a variety of companies and are used in a variety of settings. To administer various services, fog computing must be able to interact with and collaborate with a variety of suppliers or service providers.

Nebulous computing has security concerns as a young field of study, with few tools in place to detect and prevent malicious attacks on its design. Confidential nebulous computing entails identifying data and encrypting each block of data using services such as public key infrastructure. Even isolated data is sent independently to the Tooth node, which decrypts and reassembles data packets. To limit risk, the system also has the ability to restrict functionalities to reduce data interaction with fog nodes. According to their design and needs, authentication in the nebulous computing architecture is based on the existing state of authentication, no demanding authentication, and no necessary secure communication protocols. The Fog platform evaluates security and performance issues as well as entirely homomorphic processes such as cryptographic approaches [27].

CONCLUSION TO CHAPTER 3

Based on the previously reviewed and analyzed information, in order to put into practice the knowledge based on the platform, 3 architectures of the Internet of Things were developed based on the LoRaWAN protocol. The purpose of the architectures is to bring the

benefits and advantages of Fog Computing and the IoT Protocol, namely to solve energy efficiency problems, speed up calculations and data transfer speeds, and increase information security through technical aspects, protocols and Fog Computing programs. Three network architectures based on the LoRaWAN protocol were demonstrated, with a detailed description and analysis that was selected and taken on the basis of benefits and advantages, as well as close integration with Fog Computing. I can recommend this protocol because of its low power consumption, long equipment life and simple network. The Raspberry Pi 4 minicomputer was used to demonstrate the capabilities of this type of computing, as it offers sufficient computing power to work with the network and application server at a relatively low cost.

CONCLUSION

In the course of the thesis the Internet of Things was considered and the Internet of Things was introduced. The advantages for the household and the producer from the introduction of this technology and the ways of its introduction are analyzed.

Mobile services, as well as many other wireless applications, are thriving in sectors such as smart cities, healthcare, cyberphysical systems, intelligent transportation systems and the Internet of Things. Of course, wireless networks need to be scalable to meet ever-increasing needs. I can draw some conclusions based on typical approaches in this area:

The number of connected items is growing rapidly. This improves the developer's ability to create modern applications that take advantage of the ubiquitous sound and computing power of the device.

By sharing the processing load between available platforms and making extensive use of existing infrastructure, you can use network-wide computing resources to improve the performance of IoT-based applications.

The concepts and basics of the Internet of Things are considered. Today, this is a very common and relevant topic, both for ordinary life and for companies with production, which with active distribution can improve life and automate most simple processes.

Despite recent advances, the proper distribution of workload remains a challenge, as does the lack of formalization and harmonized methods for creating true common applications for IoT contexts.

The structure of cloud computing is determined, among which Computing Fog is allocated for the efficiency and security of the Internet of Things. The influence and performance of these calculations are analyzed.

Therefore, the study described here is a step forward in the development of integrated IoT and Fog applications through the distribution of software load between IoT devices.

To demonstrate the integration of Fog Computing into the Internet of Things, three network architectures based on the LoRaWAN protocol were developed and compared. These architectures can improve computing and data rates, address energy efficiency, and

improve information security through the technical aspects of Fog Computing. Cases of experimental tests with demonstration of increase in speed of action are considered. Combining cloud computing with the Internet of Things is the next big step forward in the evolution of the Internet. New IoT-Fog projects full of this combination open up new commercial and research opportunities.

In most cases, I would recommend the LoRaWAN standard because of its openness, low power consumption, long equipment life, flexibility of solutions and, most importantly, network simplicity, which, in my opinion, can really make LoRaWAN an almost ideal IoT standard. and one of the best solutions for many. This protocol is closely integrated with Fog Computing, which brings the benefits of this technology.

REFERENCES

1.Що таке «інтернет речей»? [Електронний ресурс] – Режим доступу до ресурсу: http://thefuture.news/iot/.

2. Akshat S. Application of Data Mining Techniques in IoT: A Short Review [Електронний ресурс] / S. Akshat, B. Aakash, B. Jitendra – Режим доступу до ресурсу: https://www.semanticscholar.org/paper/Application-of-Data-Mining-Techniques-in-IoT%3A-A-Savaliya-Bhatia/f7ab7fd1e41d5a1767c2ee3f479ed5bfaaf10160bfaaf10160.

3. Internet of Things, IoT [Електронний ресурс] – Режим доступу до ресурсу: https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot.

4. Abdmeziem M. R. Architecting the Internet of Things: State of the Art / M. R. Abdmeziem, D. Tandjaoui, I. Romdhani.

5. Sethi P. Internet of Things: Architectures, Protocols, and Applications [Електронний ресурс] / P. Sethi, S. Sarangi. – 2017. – Режим доступу до ресурсу: https://www.hindawi.com/journals/jece/2017/9324035/.

6. A survey on Internet of Things architectures [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S1319157816300799.

7. Atzori L. SIoT: Giving a Social Structure to the Internet of Things [Електронний ресурс] / L. Atzori, A. Iera, G. Morabito – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/6042288.

8. Internet of Things: Architectures, Protocols and Standards / S.Cirani, G. Ferrari, M. Picone, L. Veltri., 2018. – 408 p.

9. Quek T. The advantages and disadvantages of Internet Of Things (IoT) [Електронний ресурс] / Tommy Quek – Режим доступу до ресурсу: https://www.linkedin.com/pulse/advantages-disadvantages-internet-things-iot-tommy-quek.

10. Поняття хмарних обчислень: основні моделі та характеристики [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://onbiz.biz/cloud-computing-models/.

11. Хмарні обчислення [Електронний ресурс] – Режим доступу до ресурсу: http://integritysys.com.ua/solutions/pricatecloud-solution/.

12. Хмарні обчислення проти туманних обчислень [Електронний ресурс] – Режим доступу до ресурсу: https://uk.education-wiki.com/1378659-cloud-computing-vs-fog-computing.

13. Fog Computing and Its Role in the Internet of Things [Електронний ресурс] / F. Bonomi, R. Milito, J. Zhu, S. Addepalli – Режим доступу до ресурсу: https://conferences.sigcomm.org/sigcomm/2012/paper/mcc/p13.pdf.

14. Aazam M. Fog Computing and Smart Gateway Based Communication for Cloud of Things [Електронний ресурс] / M. Aazam, E. Huh – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/6984239.

15. Difference Between Edge Computing and Fog Computing [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.geeksforgeeks.org/difference-between-edge-computing-and-fog-computing/.

16. Understanding Fog Computing vs Edge Computing [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://www.onlogic.com/company/io-hub/fog-computing-vs-edge-computing/#.

17. Fog Computing in the Internet of Things. Intelligence at the Edge / Amir M. Rahmani, Pasi Liljeberg, Jürgo-Sören Preden, Axel Jantsch., 2018.

18. Fog Computing Architecture [Електронний ресурс] – Режим доступу до ресурсу: https://www.educba.com/fog-computing-architecture/.

19. Sridharan M. How Fog Computing Powers AI, IoT, and 5G [Електронний ресурс] / Madhavan Sridharan. – 2019. – Режим доступу до ресурсу: https://www.datastax.com/blog/how-fog-computing-powers-ai-iot-and-5g.

20. Combining Fog Computing and LoRaWAN Technologies for Smart Cities Applications Sobhi, Salma; Ali, Maged A.; Abdelkader, Mohamed F. https://www.econstor.eu/bitstream/10419/201754/1/ITS2019-Aswan-paper-64.pdf

21. Salma S. Combining Fog Computing and LoRaWAN Technologies for Smart Cities Applications [Електронний ресурс] / S. Salma, A. Maged, A. Mohamed. – 2019. – Режим доступу до ресурсу: https://www.econstor.eu/bitstream/10419/201754/1/ITS2019-Aswan-paper-64.pdf.

22. Jalowiczor J. Study of the Efficiency of Fog Computing in an Optimized LoRaWAN Cloud Architecture [Електронний ресурс] / J. Jalowiczor, J. Rozhon, M. Voznak. – 2021. – Режим доступу до ресурсу: https://www.mdpi.com/1424-8220/21/9/3159.

23. LoRaWAN. Specification [Електронний ресурс] – Режим доступу до ресурсу: https://lora-alliance.org/#.

24. iC880A-SPI LoRa [Електронний ресурс] – Режим доступу до ресурсу: https://wireless-solutions.de/.

25. Metzger F. Modeling of Aggregated IoT Traffic and Its Application to an IoT Cloud [Електронний ресурс] / F. Metzger, T. Hoßfeld, A. Bauer. – 2019. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/8674845.

26. Mahmud R. Fog Computing: A Taxonomy, Survey and Future Directions [Електронний ресурс] / R. Mahmud, R. Kotagiri, R. Buyya – Режим доступу до ресурсу: http://www.buyya.com/papers/FogComputingTaxonomy.pdf.

27. Ghildiyal S. Enhancing Security of Internet of Things (IoT) using Fog Computing [Електронний ресурс] / S. Ghildiyal, A. Semwal, S. Kumar – Режим доступу до ресурсу: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3402922.