

Internet of Things - Overview

Andreea MIHAI¹, Ștefania Codruța MĂNĂILĂ², Antonio Sebastian DUMITRAȘCU³
^{1,2,3}The Bucharest University of Economic Studies, Romania
mihaiandreea17@stud.ase.ro, manailastefania17@stud.ase.ro,
dumitrascuantonio18@stud.ase.ro

Abstract: *The Internet of Things (IOT) is a paradigm that has changed the traditional way of living into one in step with technology. IoT has brought great changes in several fields such as agriculture, energy, healthcare, transportation and infrastructure. A lot has been done to improve IoT technology, but there are still study challenges (technical, political) that need to be solved to reach its full potential. The main purpose of this article is to provide an overview of what IoT means, its evolution and applicability in day-to-day life. This article discusses several aspects such as IoT architecture, IoT challenges, IoT applicability areas, importance of Big Data analytics in IoT and its evolution in the last few years. Furthermore, programming languages that can be used to create IoT-type software and small examples are presented, comparisons between them. This article will help the readers to better understand IoT, real-life applicability, evolution and overview of how to develop an IoT program using Arduino or Raspberry PI.*

Keywords: *Internet of Things (IoT), IoT architecture, IoT challenges, IoT applicability areas, importance of Big Data analytics in IoT, IoT evolution, Arduino, Raspberry PI*

1 Introduction

The term "Internet of Things" (IoT) was coined by Kevin Ashton during a presentation to Procter & Gamble in 1999. The Internet of Things is a subject still under development with technical, social and economic importance. Various consumable products, durable goods, automobiles, industrial machinery, and other common objects are being combined with Internet connectivity and advanced data analysis mechanisms with the promise of changing the way people live and work. With the large-scale deployment of IoT devices, a major change can be seen in people's daily routines. IoT is used everywhere, globally, often without people even realizing it. For consumers, new IoT products such as home process automation devices and electricity management devices have introduced the concept of "Smart home", which has become an emblem of safety and sustainability. Other devices

such as health or fitness monitoring tools are transforming the way medical services can be delivered. The Internet of Things transforms physical objects into a distributed information ecosystem between both fixed and portable devices with the goal of improving the quality of human life. IoT technology also promises to be useful to the elderly or disabled, improving their level of independence at a reasonable cost. Systems such as smart cars, smart traffic orchestrators, sensors embedded in roads and bridges, make it possible to implement the concept of "smart cities", whose main objectives are to reduce traffic and energy consumption. IoT technology also has the potential to transform agriculture, industry, energy production and distribution.

A considerable number of companies and research organizations have speculated on the potential impact of IoT on the economy over the next decade. Huawei expects 100

billion IoT connections by the year 2025. Manyika et al. estimates the potential economic impact of IoT between 3.9 and 11 quadrillion dollars annually starting in 2025, impact caused by: low device prices, advances in cloud computing, and high Internet speed. IoT is expected to contribute between 4% and 11% to global GDP by the year 2025. [1]

However, implementing the Internet of Things raises significant obstacles that could stand in the way of fulfilling its beneficial purpose. Among the risks involved in implementing IoT systems are the hacking of devices, concerns about the invasion of personal space, but skepticism associated with the idea of continuous surveillance. Also, in addition to potential security issues, other obstacles to the large-scale implementation of IoT are technical, political and legal in nature. Thus, this discussion of ‘benefit vs. risk’ along with the flow of information spread through social media make IoT a complex subject to understand.[2]

2. IoT architecture

2.1 IoT architecture based on 4 levels

The layered architecture of the Internet of Things is responsible for the collection, management, storage and processing of data resources. It incorporates 4 main levels, each playing a critical role in the successful implementation of an IoT-type system. There are other secondary levels, lower levels of complexity that help improve system performance.

The IoT architecture represents the configuration of a functional Internet of Things system, in which each component is responsible for its own set of tasks. The IoT architecture offers the systems that implement it flexibility in the process of defining their own characteristics. IoT systems are used in a wide range of

applications in almost all market segments.[3]

The basic architecture of the Internet of Things is composed of four main levels:

- Perception – The Perception level is the level where data is collected by the sensors of the devices connected to the system;
- Connectivity – The Connectivity level is responsible for data transfer and facilitates communication between devices and the system network;
- Processing – The Processing level is the level where the data resources generated by the previous levels are preprocessed and stored;
- Application – The Application level represents the level where data is analyzed and used to facilitate different business requirements such as control systems, advanced analysis, etc.

2.1.1 Perception

The main objective of the Perception layer is to transform digital / analog signals. This layer forms the foundation of the IoT infrastructure, collecting data, but at the same time being able to perform actions on the collected data. Devices connected to the Internet are the bridge between the digital plane and the physical plane.

Many types of devices, using different operating systems, are used within this tier. These devices can be grouped into three categories:

- Sensors – Sensors can be represented in different forms such as meters, pressure gauges or probes. The sensors take various data related to the environment such as temperature, pressure or wind speed and transform the information into digital signals. These signals are then transmitted to cloud platforms for processing;
- Actuators – Actuators play the opposite role of sensors. They transform the

digital signals transmitted by an IoT system into concrete actions that can be used to control the behavior of connected devices;

- Devices – Sensors and actuators are often connected to different devices. In some cases, the sensor or actuator may be the main component of the device.
- The Internet Of Things architecture presents no limitation on the type of device used within the Perception layer, nor on their proximity or geographic location. A device can be a sensor of miniature dimensions or a component of an industrial machine. They can be located at a fixed point or distributed among millions of access points in different locations.[4]

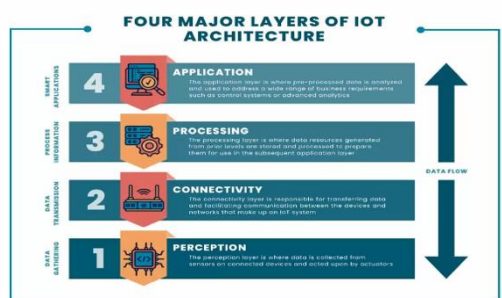


Fig. 1. IoT architecture based on four levels

2.1.2 Connectivity

The connectivity level is responsible for the communication between devices, networks and cloud systems necessary for the architecture of an IoT-type solution. The connection between the Perception layer and the Processing layer is made using the TCP/IP or UDP/IP stack. It can also be implemented using gateways that transform signals to various protocols. With the help of the gateways, it is possible to encrypt / decrypt the data transmitted within the system.

Within this level, multiple communication technologies can be used. The choice of technology used is often dependent on the

system design. Other important factors that influence the implementation of the level of connectivity are the type of devices used, the distance traveled by the signals, but also the potential obstacles that can prevent data traffic.

Among the technologies used within this level are the following:

- Ethernet – Ethernet uses cable communication to provide secure and high-speed connectivity over short distances;
- WiFi – WiFi provides wireless connectivity for short distances;
- Low-power Wide-area Network (LPWAN) – LPWAN is a technology created for IoT devices that provides low power consumption, high battery capacity and wireless connectivity for long distances;
- Cellular networks – Using cellular networks, the IoT system benefits from stable connectivity with global coverage. It involves high cost and high consumption of electricity.
- The main communication protocols used to facilitate data transport between devices and cloud platforms are:
 - Data Distribution Service (DDS) – Ensures the communication of IoT components in real time;
 - Message Queue Telemetry Transport (MQTT) – It is used in collecting data from devices with low energy consumption;
 - Constrained Application Protocol (CoAP) – It is used for devices with resource constraints;
 - Advanced Message Queuing Protocol (AMQP) – Supports the exchange of information between servers.

The optimal combination of technology and communication protocol is essential for creating an IoT architecture.

2.1.3 Processing

The Processing level is the level where the data generated within the Perception level and transmitted through the Connectivity level are collected, stored and processed. The data goes through two stages of processing within this level.

The data accumulation stage is the mechanism by which the generated data is transformed into an interpretable form for the Application layer. The purpose of this stage is to efficiently sort and store the accumulated data, making it accessible to the next level of the system. Data can be stored in different ways depending on its relevance within the system. Multiple technologies are used for IoT data persistence.

The data abstraction stage is the final stage of data preprocessing where it is beautified and abstracted for further use in applications. Data from both IoT and non-IoT sources is unified and brought to one single format. The information is then aggregated and stored centrally to facilitate quick accessibility.

The Processing layer also manages the reformatting of the data returned by the Application layer so that it can be interpreted by the devices.

2.1.4 Application

The Application layer of an IoT infrastructure is where data is analyzed to solve business requirements and meet objectives. Software tools transform data generated by the design layer into meaningful information for users or the system. APIs are used to integrate IoT software with a middleware. Certain IoT platforms offer native data visualization or analysis features.[5]

Users interact directly with the Application layer and can monitor IoT devices and track data through various tools such as

dashboards or mobile applications. This level is realized in different forms in the various areas of domains:

- Mobile phone GPSs are an example of a user-oriented IoT application;
- IoT systems can provide business intelligence solutions regarding consumer activity and market trends to facilitate enterprise decision-making;
- Robots and automated machines are also monitored and controlled through the application layer. Systems can also use machine learning techniques to increase their performance and accuracy as they are used;
- Intelligent road management systems rely on the Application layer of the IoT architecture to provide accurate information.

2.2 IoT architecture based on 7 levels

In addition to the four main layers, additional layers are used in the seven-layer IoT architecture to improve the performance of the IoT infrastructure:

- Edge or Fog computing;
- Business;
- Security;

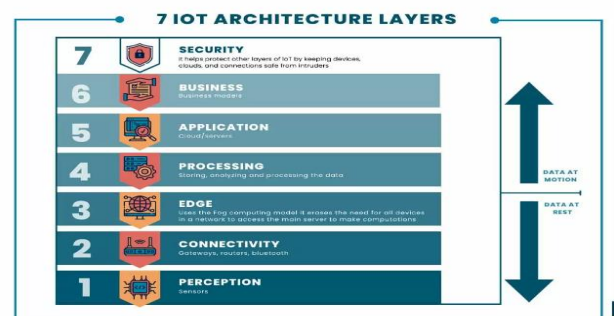


Fig. 2. IoT Architecture with 7 layers

2.2.1 Edge or Fog computing

Edge or Fog computing is designed to reduce latency and take advantage of the availability of 5G mobile networks. The objective of this level is to process and store the information as close as possible to its source, without involving its transmission

to the cloud platform. These activities are performed at the edge of the network to save time and resources needed to communicate with the cloud environment.[6]

Edge computing enables real-time processing of a considerable volume of data. In some cases, the Edge layer plays the role of both the Processing layer and the Application layer, allowing data to be transmitted directly to devices. It can also be used to analyze and evaluate data if it requires further processing or needs to be sent to another point.

2.2.2 Business

The Business layer is where solutions and decisions are drawn from the Application layer. It can contain multiple instances of the Application layer increasing its complexity and arguing the need to separate it into a distinct entity. It is the most important level for enterprises opting for an IoT infrastructure.

2.2.3 Security

E2E security is essential in any IoT infrastructure. Often, confidential data is also transmitted within a system, making security a critical component of the architecture. Compromised devices can put users' health and safety at risk. The Security layer spans all other layers of the architecture and is critical to the success of implementing an IoT solution.

Security can be sub-classified into three main categories:

1. Device Security – Security must be ensured from the very beginning, within the Perception layer. Thus, the devices must be equipped with both hardware and firmware fuses. Specific device security features include:

- Ensuring authentication by means of cryptographic keys;
- Physical protection of devices by strengthening their outer layer;
- Preventing unauthorized code from running on a connected device;

- Installing firmware to address possible vulnerabilities.

2. Connection security – Data must be secured by means of encryption at the time of its transport within the Connectivity layer. End-to-end scripting eliminates the risk of data being intercepted and used by unauthorized users.

3. Cloud Security – Cloud security is achieved by encrypting stored data to reduce the risk of disclosure of confidential information involved in a possible security breach. Access to IoT applications must be limited by implementing a set of measures aimed at authorizing and authenticating users. Devices also need to be authorized when connecting them to the IoT system to prevent unauthorized devices from connecting.[7]

Security must be the main feature in all IoT deployments. Their complexity and flexibility can often involve difficulties in securing the infrastructure. All possible security issues must be resolved before the system is put into production.

3. IoT challenges

The Internet of Things (IoT) is often hailed for its revolutionary potential in terms of application, which is why IoT devices are increasingly used in various economic sectors for varied purposes. However, there are still uncertainties about how the IoT will evolve, as it has to face some technical challenges as well as some political challenges.

3.1 Technical challenges

There are certain technical limitations that influence the development and applicability of IoT applications, such as the absence of Internet addresses within the most widely used protocol, the limited availability of high-speed wireless communications, and the lack of consensus on technical details.

3.1.1 Internet addresses

There is a significant limitation in IoT development, which lies in the technical restrictions of the Internet Protocol (IP) version most commonly used today. Internet Protocol consists of a set of standards used by computers to transmit and receive information over the Internet, including the unique address each device must be connected to in order to communicate. The predominant version of the IP protocol is IPv4, which allows for around four billion addresses, and this capacity is almost exhausted, with only a few new addresses available in various regions of the world.[8] Forecasts indicate rapid growth in Internet traffic over the next five years, largely driven by IoT technologies compared to other devices that require Internet connectivity.[9] In 2020, out of a total of approximately 50 billion devices connected to the Internet, over 25 billion were IoT devices.[10] Despite some workarounds, such as IP address sharing, it is unlikely that IPv4 will be able to meet this growing demand.

Conversely, the advent of version 6 of the IP protocol can support a significant increase in the number of available IP addresses. There is a strong likelihood that IPv6 will be widely deployed to handle the expected increase in the number of devices connected to the Internet. IPv6 has been available since 1999, but was only officially launched in 2012. By 2015, in most countries, less than 10% of IP addresses were using this version. Its spread is highest in certain European countries and in the United States of America, where it has seen an increase of up to 20% in recent years. Globally, the adoption of version 6 has doubled annually since 2011, reaching approximately 7% of all addresses in mid-2015. However, continued growth in adoption does not guarantee that IPv6 will be able to meet the evolution of IoT device usage. This depends on several factors, such as updating legacy systems and applications that cannot support IPv6 addresses,

addressing security issues associated with the transition, and the availability of development resources.[11]

3.1.2 High speed internet

It is obvious that IoT devices fundamentally require an internet connection to function effectively. This requirement can become a challenge if the Internet connection is not of high quality and telecommunication services are not advanced enough.

Although Internet access is generally available in urban and suburban environments, the situation is different in rural environments, where private service providers have difficulty installing the necessary infrastructure, as it is not considered profitable and government programs are limited.

3.1.3 Wireless communications

According to experts in the field, it is considered essential to solve the issues related to access to the electromagnetic spectrum to ensure efficient operation and interoperability of IoT devices. Access to spectrum, whether licensed or not, is crucial for wireless communication of devices and objects without the need for a physical connection. Although IoT devices are used in various industries and purposes, there are opinions that the current allocation of the electromagnetic spectrum is not adequate to meet the specific needs of IoT solutions in these fields and industries.

3.1.4 Technical standards

Currently, there is no global consensus on technical standards for the Internet of Things (IoT), especially regarding communication-related aspects, and no universally accepted definition in organizations responsible for developing standards or common documents for IoT.[12] However, the need for a set of common standards and rules is recognized to ensure the interconnectivity and

scalability of IoT devices and systems. However, there are concerns about adopting common development standards, due to the diversity of IoT devices and the specific needs of different industries and fields.[13]

3.1.5 Other technical issues

In addition to the existence of a common implementation standard, we also face other technical challenges that can limit the development of IoT applications. For example, the security and safe updating of smart objects can be an issue. It is recommended that IoT devices provide remote update capability to ensure proper security and functionality. However, there is a risk that these upgrade capabilities may have unwanted effects, such as increasing the power requirements of IoT devices or requiring the implementation of additional functionality to ensure security during the upgrade process and to avoid the risk of an attack by hackers.

Energy efficiency is a significant technical challenge when it comes to IoT devices. The functionality of these devices relies on the consumption of energy to sense, process and communicate information. Especially if the devices are located off the grid and use batteries, replacing or recharging them can become a problem, even when optimizing energy use. This problem is commonly encountered in applications involving a large number of devices or hard-to-reach locations. As a result, alternative solutions are being developed to obtain electricity, such as the use of solar or other renewable energy sources.

3.2 Political challenges

3.2.1 Privacy

Privacy in IoT is essential to prevent abuse and unauthorized disclosure of data. Significant efforts have been made to identify privacy issues and find appropriate solutions to protect both user data and the devices themselves. Bandyopadhyay and

Sen (2011) [14] contributed with some relevant solutions in this area:

- a) People usually do not agree with the idea of their data being accessible to the general public. Therefore, it is necessary to have a control over the personal information of users to ensure the confidentiality of their data.
- b) There is a strong desire that people not be tracked without their consent. However, to protect location privacy, it is necessary to have adequate control over the user's physical location and movements.
- c) In order to guarantee the right to confidentiality, it is necessary to implement standardized policies at the legislative level in this regard.
- d) To ensure effective privacy management, it is essential to develop regulated standards, methodologies and tools.

According to previous studies (Chan and Perring 2003) [15], data associated with users and devices in the IoT must be stored in authorized servers and accessible only by authorized individuals or entities. In the context of IoT systems, various entities communicate and interact, each with their own privacy policies. For this reason, conflicts and inconsistencies between these policies inevitably arise. It is thus necessary to develop new solutions to check, notify and resolve these consistency issues. Given that privacy policies are a real limitation to the effective interaction of IoT systems, there is a strong motivation for researchers to create a common and descriptive language that defines a standard set of privacy policies.

3.2.2 Security

Privacy and security are interrelated issues in the IoT field. Security is a significant challenge for physical IoT components such as wireless sensor networks (WSNs) and radio frequency identification (RFID) devices. This is due to limited resources, computational constraints, limited storage

spaces, low battery power, and other factors. As networks and sensor devices are used in sensitive applications, they are at risk of attacks in insecure environments. Any attack on one node in an IoT system can compromise the entire network of sensor nodes.

Software and hardware improvements are aimed at preventing such events in certain situations. However, to effectively manage security issues, advanced countermeasures such as vulnerable node detection techniques, encryption algorithms, encryption key management mechanisms, and secure routing protocols are required. These additional measures contribute to increasing the level of security and protection of IoT systems.

Thus, it can be seen that privacy and security are essential aspects in the field of IoT and require appropriate approaches and solutions to ensure data protection and systems functionality.

In a restricted environment where there are valuable objects or equipment, it is important to have applications that provide immediate notifications to users if they are moved or taken without permission. These applications may use various communication methods, such as SMS text messages, emails, or voice recordings, to inform the user of the unauthorized event.

Even in the presence of the risk of security attacks, IoT applications and services must be able to perform their functions and retrieve data in real time. This involves implementing appropriate security measures such as user authentication, data encryption, and activity monitoring to detect suspicious behavior.

In the event of unexpected security attacks, devices or nodes may need to be reprogrammed to fix the system. This process may involve updating software, applying security patches, or changing the configuration of devices to prevent exploitation of vulnerabilities.[16]

3.2.2.1 Data authentication

Data authentication in IoT communications is essential to avoid situations where data sent by a sender does not reach the specified receiver or to prevent unauthorized modification or interception. One of the techniques used to authenticate messages is the Hash Message Authentication Code (HMAC), according to Krawczyk (1997). [17]

HMAC is a cryptographic technique that uses a shared secret key between the parties involved in the communication. This key is used in conjunction with a hash function, such as MD5 (Message Digest Algorithm 5) or SHA (Secure Hash Algorithm), to calculate a message authentication code. This authentication code is attached to the message and can be verified by the receiver of the message using the same secret key and the corresponding hash function.

By using HMAC, messages can be securely authenticated, guaranteeing that they come from the stated source and have not been altered during transmission. The technique provides an additional level of security and integrity within IoT communication, ensuring that data is authentic and has not been compromised during transfer.

It is important to note that as technology advances, other methods of authenticating data within the IoT have been developed, such as digital certificates and advanced cryptographic protocols. These techniques can be tailored to the specific needs of the IoT system and can provide high levels of security and authentication.

3.2.2.3 Data integration

In the context of data integration in IoT systems, it is crucial to ensure the integrity of messages and verify the veracity of their sources. RFID (Radio Frequency Identification) tags, commonly used in IoT, present certain challenges in this regard, as they are often unsupervised and can be vulnerable to attack.

According to Jules (2006) [18], RFID tags may be at risk of data alteration when transferred over the network. This can be a major concern from a security perspective, as the data stored and generated by RFID tags can be manipulated by attackers, which can compromise their integrity and authenticity.

To protect the data stored in RFID tags against attacks and memory corruption, various memory protection techniques have been proposed. For example, EPCglobal class-1 and generation-2 tags use passwords to protect memory against read and overwrite operations. The memory of such a tag is divided into layers, and each layer is protected independently by using a password.

However, using passwords presents certain challenges. Often, RFID tags only support short passwords, which can compromise security. In addition, managing communication between different IoT systems becomes complex when they belong to different organizations and must rely on interoperable authentication and security mechanisms.

Consequently, ensuring the security and integrity of data in IoT systems, including the use of RFID tags, requires the implementation of robust solutions and protocols. These may involve advanced methods of encryption, authentication and access management, as well as common standards and agreements between the various systems and organizations involved in the IoT.

3.2.3 Trust and governance

Within the IoT domain, there is no general definition for the concept of trust. However, according to Blaze (1996) [19], trust can be defined as a set of policies and credentials used to manage access to resources.

According to Roman's (2011) study [20], in the IoT environment, trust mechanisms must meet certain essential requirements:

- Lowering the level of insecurity of objects when they interact with each other;
- Coordination of objects in associating with reliable partners for the fulfillment of the same purpose;
- Ensuring reliable, dynamic and cooperative environments in which the objects can carry out their activity;
- Understanding the effects that IoT systems can cause on users' sensations when they interact with them. Users must have control over their own services and must have the necessary tools to accurately describe their interactions with the IoT world;

Daubert (2015) [21] classifies trust into four categories:

- Device Trust: Supports the need to interact only with trusted devices. To achieve this purpose, reliable software products and schemes must be used;
- Trust in the process: implies the need to interact only with relevant and correct data. In this case, accurate data collection, sustainable data analysis and data fusion are required;
- Connection trust: involves the need to exchange information only with the right provider service. Here, data integration, authentication and privacy processes are required.
- Trust in the system: implies the need to interact in a general system of trust. Here the workflows must be provided in a transparent manner, the processes and technologies underlying the system and also described within the specific contexts.

4. Areas of applicability of IoT

IoT has the potential to significantly impact various sectors of the economy and society. However, the extent and nature of its evolution remain uncertain. The development of IoT is expected to bring positive benefits in terms of integration, efficiency and productivity across multiple sectors and global economies. Agriculture,

energy, healthcare, manufacturing services, and the transportation sector are among those most likely to benefit from IoT advancements. This development could have a favorable impact on economic growth, infrastructures and cities, as well as on ordinary consumers. However, there are technical and political challenges that can slow IoT development and trust, including security and privacy issues, as mentioned earlier. [22]

Various economic analyzes indicate that the IoT will contribute significantly to economic growth over the next decade, but estimates vary considerably as to the magnitude of this impact. The current IoT market has been valued at approximately two trillion dollars, and in the next five to ten years it is forecast to reach a value between four and 11 trillion dollars. The wide variation reflects the difficulty in making economic forecasts, as there are various uncertainties and no common trajectory accepted by researchers regarding the exact definition of the IoT and how it will develop in the future. Next, it's described how the influence of IoT can be felt in different economic sectors. [23]

4.1 Agriculture

Agriculture is adopting IoT technology to achieve accurate results, optimize production and efficiency, while reducing costs and the impact of climate events. IoT enables detailed analysis of real-time data collected in agricultural processes, including climate conditions, air and water quality, soil condition, water supplies, pest population, crop development, and other factors such as costs, equipment availability, and labor management.[24] For example, soil sensors are used to precisely monitor soil moisture and chemical balance.[25] These sensors can be integrated with technologies installed in different areas of crops to activate precise irrigation and fertilization. Drones and satellites are used to provide clear images of land quality, giving farmers information on

crop progress, nutrient deficiencies and the location of weeds. In animal husbandry, technologies such as radio frequency identification (RFID) chips and electronic identification tags (EID) are used to monitor animal movements, feeding and breeding patterns and generate detailed individual reports for each animal. [26]

4.2 Energy

In the energy industry, IoT technology is having a significant impact on energy production and distribution, facilitating the control of oil pipelines and wellheads, for example. When IoT components are integrated into the various parts of the power grid, an infrastructure called the "smart grid" is formed. This IoT integration enables more precise control of electricity flow and can improve the efficiency of network operations. It also facilitates the integration of microgenerators into the grid. Smart grids allow ordinary consumers to have greater control over energy consumption in homes and offices. The installation of smart meters in temperature or lighting control systems, as well as in other systems in a building, leads to the emergence of "smart buildings" that integrate the operation of these systems. Smart buildings rely on the use of sensors and data to regulate temperature, lighting and overall energy consumption, resulting in reduced energy waste and lower costs for consumers. Information collected from buildings located in a narrow area can later be integrated to achieve additional efficiency at the level of a neighborhood or a wider area of a city. [27]

4.3 The health system

IoT solutions are making a significant impact in the healthcare industry, focusing on the monitoring and treatment of conditions by providing remote medical services. These applications use medical technologies and the Internet to provide remote healthcare and education. IoT

devices, such as wearables, implantables, or ingestibles, provide information about vital signs, chronic conditions, and other indicators of health and well-being. Thus, the healthcare sector benefits from a wide spectrum of IoT devices adapted to individual needs. [28]

4.4 Manufacturing

In the industrial sector, the implementation of IoT solutions is revolutionizing manufacturing processes and supply chain logistics. Optimizing operations is one of the main benefits these applications bring, turning factories into more efficient units. By connecting components in the factory, production can be optimized, and by connecting components in the inventory and distribution process, the supply chain can be optimized. In addition, IoT applications used in this field facilitate maintenance and enable the prediction of potential failures. Sensors monitor machinery and factory infrastructure, and the data collected is used by maintenance teams to decide when to replace faulty parts, thus avoiding unwanted and costly events. [29]

4.5 Transport

In the field of transport, interconnectivity is becoming more and more present. Most motor vehicles today are equipped with GPS applications and entertainment systems, as well as driver assistance systems that use sensors for maneuvers such as parking or emergency braking. With the advancement of IoT, it is estimated that in the next 5-20 years, fully autonomous vehicles will be commercialized, capable of operating without human intervention, relying only on the interconnectivity of the vehicle's systems. [30]

In addition, IoT technologies enable the interconnection of vehicles of various categories, including cars, buses, trains, airplanes, and drones, to form an Intelligent Transportation System (ITS). This system

facilitates communication between vehicles and IoT infrastructure components, resulting in the prevention of accidents, optimization of traffic flow, saving of energy resources and reduction of associated costs. [31]

4.6 Infrastructure and smart cities

IoT infrastructure can be implemented in various sectors of public utilities, including sewage, water transport and treatment, public transport and waste management, helping to create an integrated and efficient infrastructure, especially in the urban environment. For example, traffic management authorities can use cameras with built-in sensors to monitor and regulate traffic flow, thereby reducing congestion. IoT components integrated into public lighting or other elements of street infrastructure can provide advanced lighting control functionality, environmental monitoring and easy parking assistance. In addition, smart waste containers can communicate with public cleaning teams when they are full, thus optimizing collection routes. [32]

In the context of smart cities, the integration of infrastructure components with services has led to the development of a complex concept. There is still no standard definition or rules that clearly characterize such a city, as the characteristics can vary considerably. In general, the smart city concept refers to the use of IoT technologies to improve energy consumption, transportation processes, governance and other public services in order to meet specific needs and promote sustainability and improve the quality of life. Technologies IoT communicates with include: [33]

- Virtual social networks, such as Facebook or Twitter, which facilitate interaction between city residents and local authorities, as well as the exchange of information and opinions.
- Mobile devices, such as phones and smart watches, which allow easy access to information and services, such as

interactive maps, public transport schedules or mobile payment services.

- Data analysis, which involves the processing and use of large volumes of information (the phenomenon of big data) and the use of public and widely accessible databases (open data) to obtain relevant information and make more informed decisions regarding urban planning, resource management or energy efficiency.
- Cloud computing, which involves the distribution of computing and storage services to a remote infrastructure, thus offering the possibility to access and use resources in a flexible and scalable way.

5. Importance of Big Data analytics in IoT

Big Data plays an important role in the field of IoT (Internet of Things) as it enables organizations to collect, analyze and interpret large amounts of data generated by IoT devices. IoT has also revolutionized the way we live and work, and this aspect refers to the network of physical devices, vehicles, buildings and other elements embedded with sensors, software and network connectivity that enable them to collect and exchange data. The high volume and variety of data generated by these devices presents significant challenges for analysis and decision-making. This is where big data analysis comes in.

Big data analytics refers to the process of analyzing large and complex data sets to uncover hidden patterns, correlations, and insights. Some of the key reasons why big data is important in IoT are: [34]

1. Data collection and management: IoT devices generate large amounts of data, which can be difficult to manage and analyze without the use of big data technologies. Using big data tools and platforms, organizations can effectively collect, store and manage data from IoT devices.

In general, there are three main stages of the data collection and management process in IoT:

a) Data collection - This involves capturing and collecting data from IoT devices such as temperature, humidity or pressure sensors. This data is often collected through wireless communication technology such as Wi-Fi, Bluetooth or cellular networks.

b) Data processing - After data is collected, it must be processed before it can be used. This process involves processing raw data into an usable format, such as converting the data to digital format, and then applying algorithms and analysis models to generate valuable insights.

c) Data management - The processed data is then stored in a centralized system such as a cloud server. This data must be managed in a secure and reliable way to avoid its loss or corruption. This involves the use of security technologies and tools to protect data against cyber-attacks and other threats.



Fig. 3. Big Data characteristics

In addition, there are several aspects of data collection and management in the IoT that need to be considered, including:

Large volume of data - With billions of connected IoT devices, the volume of data generated is enormous. This can lead to difficulties in data management and processing.

Data Quality - Data collected from IoT devices can be inaccurate or incomplete, which can affect the value of the information obtained through data analysis. It is important to ensure good data quality

by using high quality sensors and by validating the data before processing.

Data Integrity - Data collected in IoT must be managed in a secure and reliable way to avoid its loss or corruption. This involves the use of security technologies and tools to protect data against cyber-attacks and other threats.

In general, data collection and management in IoT are critical processes to be able to get the maximum benefits from this field.

2. **Real-time analysis:** Big data technologies enable real-time analysis of data, which is essential for IoT applications that require real-time decision making. For example, in a smart city application, real-time analytics can help city officials respond quickly to traffic congestion or other issues.
3. **Predictive analytics:** IoT devices can collect data about their own performance and usage, which can be used to predict when maintenance is needed. Big data analysis of historical data collected from IoT devices can help organizations develop predictive analytics models to analyze this data to identify patterns and predict/anticipate and prevent potential equipment failures before they occur, reducing downtime and costs. For example, this type of predictive analytics can be applied in manufacturing.
4. **Improved customer experience:** By analyzing big data from IoT devices, organizations can gain insights into customer behavior and preferences, which can be used to provide insights and recommendations based on large and complex data sets. For example, retailers can use data from IoT devices to better understand customer behavior and preferences, allowing them to develop their products, personalize their services and improve the customer experience, leading to a stronger relationship between companies and customers.
5. **Enhanced Security:** IoT devices can be vulnerable to cyber-attacks, and big data analytics can help organizations detect and respond to these threats in real time.

By analyzing data from multiple sources, organizations can identify patterns and anomalies that may indicate a security breach.

Data security in IoT is essential to protect confidential information and prevent data loss or corruption. By implementing appropriate security measures, the protection of sensitive data can be ensured and the maximum benefits of big data analytics in IoT can be obtained.

An IoT system comprises a large number of devices and sensors that communicate with each other. With the expansion of IoT, the number of sensors and devices is growing rapidly. These devices communicate with each other and transfer large volumes of data over the Internet. This data is very large and is transmitted every second and hence it is called "big data". The continuous expansion of IoT-based networks gives rise to complex issues such as data management and collection, storage and processing and analysis. The large amount of IoT data for smart buildings is very useful to deal with several issues of smart buildings, such as managing oxygen levels, measuring smoke/hazardous gases and brightness. Such a framework is able to collect data from sensors installed in buildings and perform data analysis for decision making. In addition, industrial production can be improved using an IoT-based cyber-physical system that is equipped with information analysis and knowledge acquisition techniques. Traffic congestion is an important issue in smart cities. Real-time traffic information can be collected through IoT devices and sensors installed in traffic signals, and this information can be analyzed in an IoT-based traffic management system. In healthcare analytics, IoT sensors used with patients generate a wealth of information about patients' health every second. This large amount of information must be integrated into a single database and must be processed in real time to make quick decisions with high accuracy, and big data technology is the best solution for this job. IoT along with

big data analytics can also help transform the traditional approaches used in manufacturing industries into a modern one. Sensing devices generate information that can be analyzed using big data approaches and can help with various decision-making tasks. In addition, the use of cloud computing and analytics can benefit the development and conservation of low-cost energy and customer satisfaction. IoT devices generate a huge amount of streaming data that needs to be stored efficiently, additional analytics for real-time decision making. Deep learning is very efficient to deal with such a large amount of information and can provide results with high accuracy. Therefore, IoT, Big Data Analytics and Deep learning together are very important to develop a high-tech society.

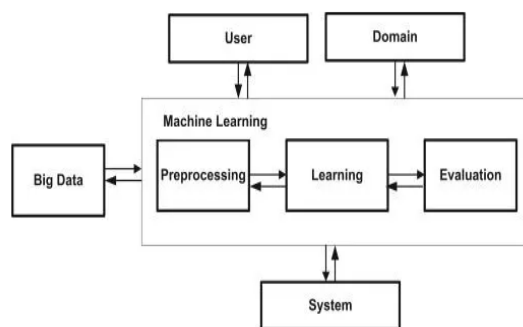


Fig. 4. IoT, Big Data and Machine learning interaction

In conclusion, big data analytics is critical to IoT as it enables organizations to extract meaningful insights from the large amounts of data generated by IoT devices. It enables organizations to monitor, analyze and respond to real-time data, predict potential problems, improve decision-making and enhance security.

6. The evolution of IoT in the last few years

In the last few years, the Internet of Things (IoT) has experienced a significant evolution, being considered one of the most important trends in the field of technology.

One of the key factors contributing to the evolution of IoT has been the development of connectivity technology such as 5G and Wi-Fi 6, which have increased the speed and capacity of data transmission. This has allowed IoT devices to communicate more efficiently and collect and transmit more data in real time.

In addition, the evolution of sensor technology has led to the development of smaller and more efficient IoT devices that can be used in various fields such as health, agriculture or manufacturing. For example, sensors can be used to collect data on the health status of patients, monitor crops and improve the efficiency of production processes.

Another important trend in the evolution of IoT is the increased use of data analytics, especially predictive analytics and artificial intelligence. These technologies enable IoT devices to collect and analyze data in real time, providing valuable insights and automated actions such as alerting users or adjusting device settings.

In conclusion, the IoT has experienced significant evolution in recent years due to the development of connectivity and sensor technology, as well as the increased use of data analytics and artificial intelligence. This evolution has enabled IoT devices to become more efficient and useful in various fields, thereby improving the quality of people's lives and the efficiency of industrial processes.

With the evolution of IoT in recent years, this has even started to be taught to children. Teaching IoT to children is an important initiative that helps them understand how technology works and how it can be applied in different fields such as industry, health, agriculture or household. Learning about IoT can give children a wider perspective on the world of technology and help develop their skills in an interactive and creative way.

There are different approaches in teaching IoT to children, such as using games and interactive experiments to make children understand the basic concepts of IoT and

apply them in practical activities. For example, children can build a simple IoT device, such as a temperature sensor, and learn how to collect and analyze the resulting data.

In addition, teaching IoT to children can help develop digital skills such as programming, design and analytical thinking. These skills are important in today's digital age and are needed to face future challenges in career and personal life. Teaching IoT to children can also help develop teamwork and collaboration skills, as IoT projects often require collaboration between different people with different expertise.

In conclusion, teaching IoT to children can have multiple benefits, such as developing digital skills, team and collaboration skills, and their ability to understand and apply technology in different fields.

There are a variety of IDEs (Integrated Development Environments) available for developing IoT applications, which are designed to facilitate the process of programming and testing IoT devices and applications. Below are some examples: [35]

1. Arduino IDE - is an open source platform, used for the development and programming of Arduino microcontrollers. It is a popular and easy-to-use solution for novice developers.

2. Eclipse IoT - is a suite of development tools, including Eclipse Kura, Eclipse Paho and Eclipse SmartHome. Eclipse Kura is an IoT gateway platform and Eclipse Paho is an MQTT client library. Eclipse SmartHome is an open source platform for developing smart home automation solutions.

3. Visual Studio Code - is an open source code editor developed by Microsoft that supports the development of IoT applications. It can be used to develop IoT applications for devices like Raspberry Pi and Arduino.

4. PlatformIO - is an open source platform that supports the development of IoT applications for a wide range of devices,

including Arduino, ESP8266, ESP32 and Raspberry Pi.

5. Particle IDE - is a cloud-based IoT application development platform that supports the development and testing of applications for Particle devices.

These are just a few examples of IDEs for IoT application development. In general, IDEs must support IoT device programming, application development, testing, and debugging. It should also be easy to use and support a wide range of devices and platforms.

Arduino and Raspberry Pi are popular platforms for building electronic projects and creating interactive devices. However, they have some key differences.

Arduino is a microcontroller board that is designed to build simple electronic projects. It has a small form factor and is easy to use, even for beginners. The Arduino board contains a microcontroller chip, which is programmed using the Arduino software. Arduino is great for projects that require precise timing or need to interact with physical sensors or actuators.

Raspberry Pi, on the other hand, is a single-board computer that runs a full operating system (such as Linux). It is more powerful than an Arduino and can handle more complex tasks such as running a web server or media center. The Raspberry Pi also has built-in Wi-Fi and Bluetooth connectivity, making it easy to connect to other devices and the internet.

In short, if one wants to build a simple electronic project that interacts with physical sensors or actuators, Arduino is a good choice. If one wants to build a more complex project that requires computing power, connectivity and the ability to run a full operating system, then the Raspberry Pi may be a better choice.

Raspberry Pi	Arduino
Microcomputer	Microcontroller
Needs an operating system	Does not need an operating system
Complicated	Simple
Video out, Camera, Ethernet ports, Wifi, Bluetooth, USB, I2C, SPI, UART etc. on board	USB only for power and serial in/out, I2C, SPI, UART
Best for general computer	Best for small tasks that constantly repeat
Capable of performing a huge range of tasks	Optimised for sensing and controlling the world around it
Best for more advanced makers	Best for beginners
Programmed in many languages, including C/C++, Python, Ruby	Programmed in C/C++
Relatively high power consumption	Relatively low power consumption


Raspberry Pi Full Stack 

Fig. 5. Differences between Raspberry Pi and Arduino

```
int led=7;
// Funcția de setare (inițializare)
void setup() {
// inițializare pin digital 7 ca o ieșire.
pinMode(led, OUTPUT);
}
// funcția de buclă infinita
void loop() {
digitalWrite(led, HIGH); // pornește (scrie digital)
LED- (HIGH este nivelul de tensiune)
delay(1000); // așteapta o secundă
digitalWrite(led, LOW); // pornește (scrie digital)
LED- (LOW este nivelul de tensiune)
delay(1000); // așteaptă o secundă
}
```

Fig. 6. Script written in Arduino IDE using C programming language

In the academies where programming courses are taught to children, because they do not have the level of thinking/analysis very well developed and the necessary practice, the initiation is started in building such projects using Arduino as a board and Arduino IDE for writing the code.

Example script for lighting an LED written in Arduino IDE for Arduino and Python for Raspberry Pi:

Through the script above, the LED turns on for one second, then stays off for one second. The operation is repeated ad infinitum. [36]

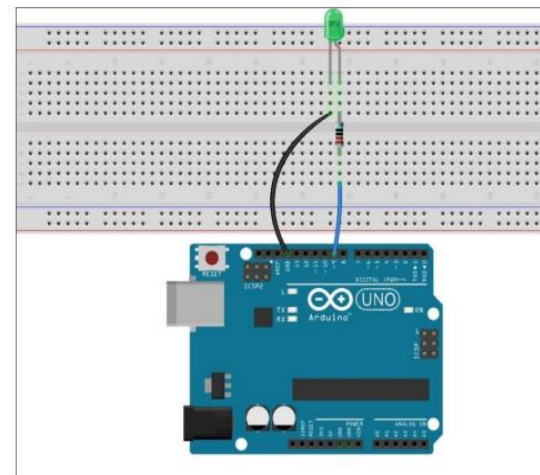


Fig. 7. Hardware schema for lighting a led

```
python
import RPi.GPIO as GPIO
import time

GPIO.setmode(GPIO.BOARD)
GPIO.setup(11, GPIO.OUT)

while True:
    GPIO.output(11, GPIO.HIGH)
    time.sleep(1)
    GPIO.output(11, GPIO.LOW)
    time.sleep(1)
```

Fig. 8. Written script in Python for Raspberry Pi

This code starts by setting the GPIO mode to board mode and configuring pin 11 as an output. It then uses an infinite while loop to turn the LED on and off repeatedly, with a 1 second delay between each state. The LED should be connected between pin 11 and a resistance of about 220 ohms and to ground. [37]

It is important not to connect the LED directly to the Raspberry Pi without a resistor, as this can cause the GPIO pin to burn.

In conclusion, Arduino and Raspberry Pi are two different platforms, each with its own advantages and disadvantages. Arduino is better for simple electronics projects that require precise timing and interaction with physical sensors or actuators, and Raspberry Pi is better for more complex projects that require

computing power, connectivity, and the ability to run a full operating system. In general, Arduino is easier to use and more beginner-friendly, while Raspberry Pi offers more flexibility and more processing power for more advanced projects. Depending on the project, the choice between the two depends on the specific requirements and available resources.

7. Conclusions

Recent technological advancements in the field of IoT expertise have attracted the attention of the international community of researchers and software developers. IoT developers are working together with researchers to expand the scalability of this new type of technology and to potentiate its benefits to society to the highest possible level. However, improvements and progress are only possible if the current unaddressed issues involved in the widespread use of IoT systems are resolved. In this scientific article, both the current context of IoT technology and the problems and challenges encountered by developers in the process of building an optimal Internet of Things model were presented. This technology not only brings benefits to various branches of human activity, but is also a way to gather unlimited amounts of data. Therefore, Big Data Analytics is also a critical factor to consider in order to build an optimal IoT model.

References

- [1] "Internet of Things (IoT)" <https://www.scirp.org/journal/paperinformation.aspx?paperid=108574>
- [2] "IoT Architecture" [Online]. Available: <https://www.javatpoint.com/iot-architecture-models>
- [3] "IoT Architecture Guide. Major and additional layers of IoT system" [Online]. Available: <https://www.helpwire.app/blog/iot-architecture/>
- [4] "What is IoT Architecture?" [Online]. Available: <https://www.mongodb.com/cloud-explained/iot-architecture>
- [5] "IoT Architecture – Detailed Explanation" [Online]. Available: <https://www.interviewbit.com/blog/iot-architecture/>
- [6] "IoT Architecture: Complete Explanation with Examples" [Online]. Available: <https://www.celona.io/network-architecture/iot-architecture>
- [7] "IoT Architecture" [Online]. Available: <https://www.javatpoint.com/iot-architecture-models>
- [8] "It's official: North America out of new IPv4 addresses" [Online]. Available: <https://arstechnica.com/information-technology/2015/07/us-exhausts-new-ipv4-addresses-waitlist-begins/>
- [9] "Cisco Annual Internet Report" [Online]. Available: <https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html>
- [10] "The Internet of Things How the Next Evolution of the Internet Is Changing Everything" [Online]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
- [11] "The Internet of Things: Frequently Asked Questions" [Online]. Available: <https://sgp.fas.org/crs/misc/R44227.pdf>
- [12] "A guide to the confusing Internet of Things standards world" [Online]. Available: <https://www.networkworld.com/article/2456421/a-guide-to-the-confusing-internet-of-things-standards-world.html>
- [13] "The state of IoT standards: Stand by for the big shakeout" [Online]. Available: <https://techbeacon.com/app-dev-testing/state-iot-standards-stand-big-shakeout>
- [14] Bandyopadhyay, D. and Sen, J. (2011) 'internet of things: applications and challenges in technology and standardization', Wireless Personal Communications, Vol. 58, No. 1, pp. 49-69
- [15] Chan, H. and Perrig, A. (2003) 'Security and privacy in sensor networks', IEEE Computer, Vol. 36, No. 10, pp. 103-105

- [16] "Internet of Things: A Survey of Challenges and Issues" [Online]. Available: - https://www.researchgate.net/publication/322603292_Internet_of_Things_A_Survey_of_Challenges_and_Issues
- [17] Krawczyk, H., Bellare, M. and Canetti, R. (1997) 'HMAC: keyed-hashing for message authentication', IETF RFC
- [18] Juels, A. (2006) 'RFID security and privacy: a research survey', IEEE Journal on Selected Areas in Communications (J-SAC)
- [19] Blaze, M., Feigenbaum, J. and Lacy, J. (1996) 'Decentralized trust management', IEEE Symposium on Security and Privacy, pp. 164-173
- [20] Roman, R., Najera, P. and Lopez, J. (2011) 'Securing the internet of things', IEEE Computer, Vol. 44, No. 9, pp. 51-58
- [21] Daubert, J., Wiesmaier, A. and Kikiras, P. (2015) 'A view on privacy & trust in IoT', The IEEE International Conference on Communication Workshop (ICCW), pp. 2665-2670
- [22] National Security Telecommunications Advisory Committee, "NSTAC Report to the President on the Internet of Things," November 19, 2014
- [23] "The Internet of Things Will Thrive by 2025" [Online]. Available: <https://www.pewresearch.org/internet/2014/05/14/internet-of-things/>
- [24] "Surprise: Agriculture is doing more with IoT Innovation than most other industries" [Online]. Available: <https://venturebeat.com/business/surprise-agriculture-is-doing-more-with-iot-innovation-than-most-other-industries/>
- [25] "Imagery: Which Way Is Right For Me?" [Online]. Available: <https://www.globalagtechinitiative.com/in-field-technologies/imagery/imagery-which-way-is-right-for-me/>
- [26] "Internet of cows: technology could help track disease, but ranchers are resistant" [Online]. Available: <https://www.theverge.com/2013/5/10/4316658/internet-of-cows-technology-offers-ways-to-track-livestock-but>
- [27] "Smart Grid. Department of Energy" [Online]. Available: <https://www.energy.gov/smart-grid>
- [28] Manyika et al., "The Internet of Things: Mapping the Value Beyond the Hype."
- [29] Macaulay, Buckalew, and Chung, "Internet of Things in Logistics."
- [30] "Autonomous Vehicle Technology" [Online]. Available: https://www.rand.org/pubs/research_reports/RR443-2.html
- [31] "USDOT's Intelligent Transportation Systems (ITS) Strategic Plan 2015-2019" [Online]. Available: <https://www.its.dot.gov/strategicplan.pdf>
- [32] "NAED-Big-Data.pdf" - [Online]. Available: <https://cdn2.hubspot.net/hubfs/2859863/Research%20Report%20Downloads/NAED-Big-Data.pdf>
- [33] "Smart cities" meet "anchor institutions": the case of broadband and the public library. [Online]. Available: <https://www.thefree-library.com/%22Smart+cities%22+meet+%22anchor+institutions%22%3A+the+case+of+broadband+and...-a0403061636>
- [34] "Big Data and IoT: Benefits, Challenges, Use Cases" [Online]. Available: <https://anywhere.epam.com/business/big-data-analytics-and-internet-of-things>
- [35] "Best IoT Development Tools" [Online]. Available: <https://www.g2.com/categories/iot-development-tools>
- [36] "Blink" [Online]. Available: <https://docs.arduino.cc/built-in-examples/basics/Blink>
- [37] "HOW TO CONTROL LEDS WITH THE RASPBERRY PI AND PYTHON" [Online]. Available: <https://www.circuitbasics.com/how-to-control-led-using-raspberry-pi-and-python/>



Andreea MIHAI – student at Bucharest University of Economic Studies, attending Data Bases – Support for Business Master, Bucharest, Romania; obtained a Bachelor’s Degree in Economic Informatics in 2021.



Ștefania – Codruta MANAILA – student at Bucharest University of Economic Studies, attending Data Bases – Support for Business Master, Bucharest, Romania; obtained a Bachelor’s Degree in Economic Informatics in 2021.



Antonio – Sebastian DUMITRASCU – student at Bucharest University of Economic Studies, attending Data Bases – Support for Business Master, Bucharest, Romania; obtained a Bachelor’s Degree in Economic Informatics in 2021.