ELECTRONICS AND IOT ARCHITECTURES FOR ENHANCED SMART TEXTILES

C.S. dr. ing. **Octavian-Adrian TABĂRĂ**

National Research and Development Institute for Textiles and Leather,
Bucharest, Romania.

REZUMAT. Internetul Lucrurilor (IoT) reprezintă un ecosistem tehnologic complex, bazat pe integrarea senzorilor, microcontrolerelor, modulelor de comunicație și a actuatorilor în infrastructuri distribuite, capabile să colecteze, să prelucreze și să transmită date în timp real. Această lucrare analizează evoluția, structura și fundamentele tehnologice ale sistemelor IoT, punând accent pe componentele electronice și pe arhitecturile care fac posibile mediile moderne interconectate. Este urmărită dezvoltarea IoT, de la primele rețele de senzori militari și sisteme SCADA până la infrastructurile actuale distribuite, îmbunătățite cu inteligență artificială, capabile de achiziție și prelucrare a datelor în timp real, precum și de luare autonomă a deciziilor. Un accent deosebit se pune pe arhitecturile IoT, fiind discutate provocări legate de interoperabilitate, gestionarea volumelor mari de date (big data) și securitatea cibernetică, alături de câteva soluții emergente. Un alt aspect important îl constituie integrarea electronicelor flexibile, a fibrelor conductive și a senzorilor miniaturizați în țesături și textile inteligente, pentru a permite aplicații în domenii precum asistența medicală, reabilitarea, siguranța industrială și moda. Convergența dintre IoT și textilele inteligente stimulează dezvoltarea următoarei generații de sisteme autonome, inteligente și ecologice.

Cuvinte cheie: microcontroler, materiale textile, rețea.

ABSTRACT. The Internet of Things (IoT) represents a complex technological ecosystem, based on the integration of sensors, microcontrollers, communication modules and actuators in distributed infrastructures capable of collecting, processing and transmitting data in real time. This paper examines the evolution, structure, and technological foundations of IoT systems, emphasizing the electronic components and architectures that enable modern connected environments. It traces the development of IoT from early military sensor networks and SCADA systems to today's distributed, AI-enhanced infrastructures capable of real-time data acquisition, processing, and autonomous decision-making. A central focus is placed on IoT architectures discussing challenges related to interoperability, big data management, and cybersecurity, along with some emerging solutions. Another important point is embedding flexible electronics, conductive fibers, and miniaturized sensors into fabrics and smart textiles to enable applications in healthcare, rehabilitation, industrial safety, and fashion. The focus on IoT and smart textiles as converging fields is driving the next generation of autonomous, intelligent and environmentally conscious systems.

Keywords: microcontroller, fabrics, network

1. INTRODUCTION

Like many other technologies, wireless sensor networks (WSNs) were originally used for military purposes. Now, however, they have expanded to include a wide range of applications, from smart homes and buildings to air quality monitoring. The first initiative that resembled wireless sensor networks was the acoustic signal-based surveillance system, known as SOSUS, developed by the U.S. military during the Cold War to detect and track Soviet submarines. This system is still active today, being used to study marine life and volcanic activities. In the 1980s, SCADA networks appeared, which dealt with supervised control and data acquisition, considered the first generation of networks implementing machine-to-machine communication (M2M).

These networks allowed interaction between two devices or objects, either through a wireless or wired communication channel. Both types of technologies make it easy to connect telemetry devices and actuators for remote management of industrial processes. A major difference between SCADA and WSN is that SCADA systems are isolated and use proprietary technologies, while WSN allows systems to be interconnected through open technologies.

Since 2008-2009, often considered the year when the Internet of Things (IoT) began, this concept has evolved alongside WSN (wireless sensor networks) networks. The IoT system is based on connecting devices to the internet, allowing them to communicate with each other and with central systems. It is usually a network for collecting, processing and transferring information in real time,

in a digital format. The sensors or actuators of each IoT-connected device generally capture information about the environment. The data collected flows through networks and is transformed into useful information. In most cases, devices act automatically. This form of machine intelligence can be simple (e.g. an LED sensor) or complex (e.g. machine learning). So, the Internet of Things supports a variety of industries globally, including: Pharmaceutical Industry – telemedicine, asset protection, smart care; Manufacturing Industry – quality control, predictive maintenance, supply automation; Transportation Industry – vehicle monitoring, diagnostics and traffic management; Smart Cities – automated infrastructures, optimized energy efficiency, improved public services.

The main components of an IoT system are the microcontroller unit, sensors, actuators. There are also secondary components, such as power supplies, buttons, connectors that have the role of integrating functionality into the technical ecosystem. In order to develop efficient IoT solutions, it is essential to understand the operation and role of each component.

Figure 1 shows a microcontroller unit and integrated circuits in a package. The fundamental components of an IoT system are: the microcontroller, sensors, actuators, plus auxiliary elements such as power supplies, connectors, and communication modules.

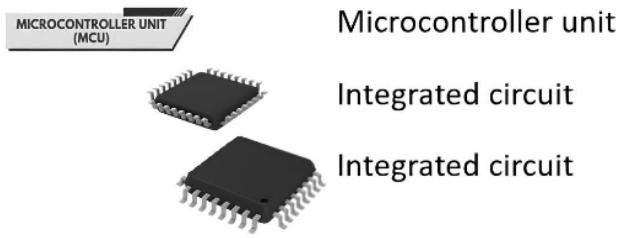


Fig. 1. Schematic example of microcontroller unit and surface-mounted circuits.

The package determines, how the chip is assembled on the board – whether it has pins for holes, cables for surface mounting, or a series of balls underneath. This choice of package is reflected throughout the board: size, thermal design, assembly process, and inspection needs. Being at the boundary between chip and board, the package is closely tied to the substrate technology of advanced parts.

So, the microcontroller unit plays an essential role in such a system. It combines a processor, memory, and input/output connections into a single chip, which allows it to execute a variety of commands. Microcontrollers come in various forms, such as QFN, TQFP, or BGA, thus offering a wide range of options for design.

Thus, QFN is a family of surface mount device component packages called QFN usually has 12-108 drifts. They are essentially small, thin-profile packages. Today, integrated circuits with a higher number of leads, such as microcontrollers, frequently use the QFN package.

TQFP is a surface-mounted integrated circuit package with piping extending from all four sides. The low profile of TQFP is a defining technical feature. Thus, it is a surface-mounted package with terminals extending from all four parts of the package.

A ball grid array (BGA), which is used in integrated circuits, is a type of surface-mounted packaging, or chip holder. Devices such as microprocessors can be permanently mounted using BGA packages. A BGA has the ability to provide more interconnect pins than a dual in-line or flat package. This is the most important connection method in modern electronics.

Microcontrollers are the ones that are in charge of data processing, device control, and managing communication between the different components. These units make intelligent decisions based on the information they receive. To turn electronic commands into concrete actions, actuators are used. These components allow systems to move, control, and display the commands for the microcontroller unit. Sensors, on the other hand, are the ones that capture the information needed for IoT applications. They provide data on temperature, humidity, motion, gases, and other environmental conditions. By converting these inputs, the sensors help the microcontroller gain valuable information [1].

2. CORE ELECTRONIC COMPONENTS OF THE IOT SYSTEM

Internet of Things devices rely on a combination of sensors, processors, communication modules, and actuators to interact with the physical world around them. Next, are presented the most important components, their roles, and how they're used in real-life IoT systems.

Electronic components are classified into: electronic circuit elements (active | passive), sensors, microcontrollers, communication modules, actuators, display modules, prototypes. This order emphasizes the levels in electronics.

2.1. Circuit elements

2.1.1. Passive components

These components do not need external energy to operate and are used to control or shape electrical signals. Details are shown in Table 1.

Table 1 **Passive components in IoT**

Component	Description	Use in IoT
Resistor	Limits the flow of current in a circuit	Protects LEDs and sensors from overcurrent
Capacitor	Stores and releases electricity	Evens out the power supply, filters signals
Inducer	Stores energy in a magnetic field	Used in power supplies and radio frequency circuits
Diode	Allows current to flow in only one direction	Protects reverse polarity circuits
Zener diode	Regulates voltage	Light detection applications, e.g. smart lighting

2.1.2. Active componets

They need power to operate and are used for amplification, switching, and processing. The active components can be found in Table 2.

Table 2 **Active components in IoT**

Component	Description	Use in IoT
Transistor	Acts as a switch or amplifier	Controls motors, relays and signal flow
IC (Integrated Circuit)	Contains multiple electronic functions	Used in sensors, controllers, and communication chips
Operational Amplifier	Amplifies voltage signals	Used in analog signal processing
Voltage regulator	Keeps the output voltage constant	Power microcontrollers safely

2.2. Sensors

Sensors act like the eyes and ears of IoT devices, converting physical phenomena into electrical signals. A detailed overview of them can be found in Table 3.

Table 3 **Sensors used in IoT**

Sensor Type	Description	Use in IoT
Temperature (e.g. LM35, DS18B20)	Measures ambient temperature	Smart thermostats, weather stations
Humidity (e.g. DHT11, DHT22)	Measures humidity in the air	Environmental monitoring
Movement (e.g. PIR)	Detect displacement	Security systems, smart lighting
Ultrasonic (e.g. HC-SR04)	Measure distance using sound waves	Obstacle detection, parking sensors
Gases (e.g. MQ-2, MQ-135)	Detects gases such as CO2, smoke	Air quality monitoring
Pressure (e.g. BMP180)	Measures atmospheric pressure	Weather forecast, altimeter
Accelerometer (e.g. MPU-6050)	Detects acceleration and slope	Wearable devices, vehicle tracking
Gyroscope	Measure orientation	Drones, robots
Magnetometer	Detects magnetic fields	Orientation Apps, Compass
Sound Sensor	Detects sound levels	Noise monitoring, voice activation
Receptor IR (infrared)	Receives infrared signals	Remote control systems
Light sensor (e.g. TSL2561)	Measures light intensity	Smart Lighting, Solar Tracking

2.3. Microcontrollers and development boards

Microcontrollers and development boards are basically the brains of IoT systems, having the role of processing data and controlling various components. A presentation of them is also in Table 4.

Table 4 **Microcontrollers and development boards used in IoT**

Plate	Description	Use in IoT
Arduino Uno	Easy-to-use microcontroller for beginners	Prototyping basic IoT projects
ESP8266	Wi-Fi compatible microcontroller	Cloud-connected devices
ESP32	Advanced microcontroller with Wi-Fi and Bluetooth	Smart homes, portable devices
Raspberry Pi	Mini computer with GPIO pins	Complex IoT systems, complex calculations

3. MODES OF COMMUNICATION

Communication modules facilitate the wireless transmission of data between devices and the cloud. A detailed description of them can be found in Table 5.

Table 5 **Communication modules used in IoT**

Module	Description	Use in IoT
Wi-Fi (ex. ESP8266)	Connects to the internet via router	Remote monitoring, cloud dashboards
Bluetooth (ex. HC-05)	Short-distance wireless communication	Portable devices, controlled mobile devices
RFID/NFC	Wireless identification	Controlled access, inventory tracking
GSM (e.g. SIM800L)	Mobile Phone Communication	SMS alerts, remote control
GPS Mode	Location tracking	Real-time vehicle tracking, geo surveying
LoRa Mode	Long-range com-munication, low power	Agriculture, smart cities

4. ACTUATORS AND OUTPUT DEVICES

Actuators control everything around us. Actuators and output devices perform actions based on the processed data. A concise overview of them is available in Table 6.

Table 6 **Actuators and output devices used in IoT**

Output devices and actuators	Description	Use in IoT
Touch screen	Displays information like a regular monitor	Navigation, selection, control without mouse/keyboard
External hard disk	Store and retrieve data	Being portable, it allows the exchange of large files
Stick USB	Store and deliver data to the system	More efficient and convenient computing, boosts productivity
Stepper motors	Translates digital pulses into mechanical motion	Robots, smart tools and automatic cutting devices
Electric motors	Turn electricity into motion	In blenders, refrigerators, fans, electric cars
Hydraulic cylinders	Generates mechanical force thanks to liquids	They perform various tasks (e.g. movement, control or manipulation) based on data received from sensors

5. DISPLAY AND INTERFACE MODULES

Display and interface modules are essential for viewing data or interacting with the electronic device. A detailed description of these can be found in Table 7.

Table 7 **Using Visualization/Interface Modules in IoT**

Component	Description	Use in IoT
LCD (16x2)	Shows text	Sensor readings, current status display
Display OLED	High-resolution display	Compact visual output
Touchable screen (touchscreen)	Data entry interface for the user	Smart panels, kiosks
Module RTC	Real-time clock	Timestamp data, task scheduling

6. PROTOTYPING TOOLS

The use of tools for prototyping is crucial for the development and testing of IoT circuits. A summary of the main components can be found in Table 8.

Table 8 **Electronic prototyping tools used in IoT**

Tool	Description	Use in IoT
Testing plate	Solderless circuit construction	Rapid prototyping
Jumper wires	Connect components to the test board	Circuit assembly
Multimeter	Measures voltage, current intensity, resistance	Troubleshooting
Soldering hammer	Permanently connect components	Final assembly
Power supply	Supply the circuits with voltage	Battery or USB-charging systems
Closures (at the end)	Protects electronics	Weatherproofing, safety

The tables previously presented, summarizes, from the author's perspective, main components in IoT systems. In short, these are the main electronic components used in any type of communication today [2].

7. ARCHITECTURES

IoT devices generate a huge amount of data. IoT devices generate big volumes of data (estimation

order is tens of zettabytes in 2025). Standardization is crucial for interoperability, security, and efficiency. This data, known as Big Data, must be collected, processed and kept safe. In addition to volume, data also faces other challenges. It is often fragmented, has variable quality, is sometimes poorly documented and is not always cleaned. This data comes from various sources: video, voice, text, images and telemetry data. In addition, access to data is no longer reserved only for specialists. The Internet of Things, being a major source of information, requires standardization and an infrastructure that allows the generation of valuable information so that data is accessible to everyone. An IoT architecture describes how data flows from the physical device all the way to the end user [3].

A common type of architecture is usually broken down into four distinct layers: 1. Perception (Edge) Layer - The physical hardware layer containing the sensors, actuators, and edge devices that interact directly with the environment, 2. Network (Transportation) Layer - The infrastructure that moves data from the edge devices to the cloud or local servers using routers, gateways, and internet protocols (like MQTT or HTTP). 3. Processing (Middleware) Layer - Where raw data is filtered, analyzed, and stored. This layer often uses cloud computing or edge servers to make sense of massive data streams. 4. Application Layer - The user-facing interface, such as a mobile app or web dashboard, where users can monitor data, view alerts, and control IoT devices remotely.

A key part of the necessary infrastructure is creating user and creator groups around specific data and topics. It all starts with identifying those who use varied data, which gives researchers, including young people and students in their final years, the opportunity to connect with other specialists in their field. Additionally, this helps government agencies and research-funded organizations understand how their data investments are being leveraged. Scientists can also discover relevant work that aligns with their research. In terms of the architecture of the Internet of Things, it is crucial to understand how smart devices communicate and function within the system. So, it is important to familiarize yourself in detail with the Internet of Things (IoT) Architecture. To achieve this, it needs to be defined how sensors, networks, and cloud systems interact to collect, process, and exchange data in an efficient way.

IoT architecture is known to function as an essential foundation for all connected devices and applications. Each layer has a specific role, from capturing real-world data to performing smart actions. A well-defined structure ensures scalability, security, and seamless communication between devices. Architecture is the backbone of IoT systems, supporting everything from smart homes to industrial automation. It is composed of four distinct layers: the Sensor Layer, the Network Layer, the Data Processing Layer, and the Application Layer, exemplified in Figure 2.

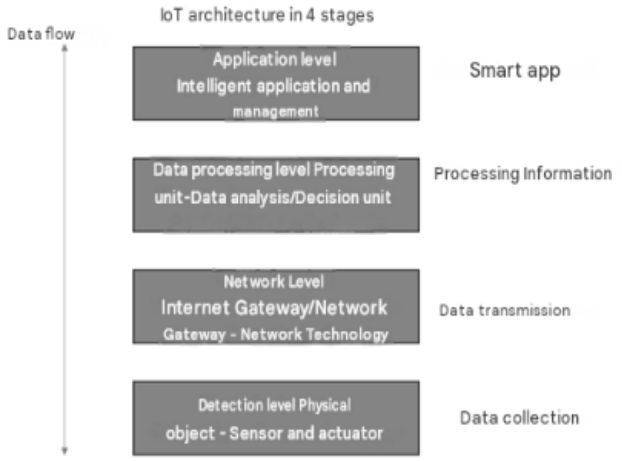


Fig. 2. IoT Architecture

7.1. Levels in IOT architecture

The architecture layers in the Internet of Things mainly comprise 4 layers: the detection layer, the network layer, the data processing layer, the application layer.

1. Detection layer

The detection layer is the lowest level, having the role of perceiving the physical conditions around us. Its functions include collecting raw data such as temperature, humidity, motion, noise and pressure. Thanks to its integrated components, this layer transforms information from the environment into quantifiable data. Another important aspect is that it can initiate Actions through actuators when necessary.

Among the components, sensors such as humidity, gas, infrared and ultrasonic can be highlighted. There are also actuators, such as motors, switches and valves, but also microcontrollers and RFID tags. In terms of communications, this layer deals with the transfer of detected data to the network layer, either through wired or wireless connections.

2. Network layer

This layer plays a critical role in providing connectivity and communication between IoT devices and cloud systems. It is in charge of transmitting the data collected by sensors to processing platforms, in a secure way. Another important function of this layer is to facilitate communication between devices and servers. It also takes care of addressing, routing, and forwarding data. The technologies used include Wi-Fi, Bluetooth, Zigbee, and LoRaWAN. In addition, Ethernet technologies and satellite networks are also used, along with supporting equipment such as routers and switches.

3. Data Processing Layer

The data processing layer is essential for analyzing, filtering, and interpreting information received from network devices. This layer is in charge of cleaning and formatting raw data from sensors, turning it into truly meaningful information. Functionally, it performs analysis to identify patterns or anomalies. Also, another important aspect of this layer is storing data for historical analysis or reporting.

Components of this layer include IoT cloud platforms, data places, and storage. Its main role is to process data streams and use machine learning engines. It also plays a crucial role on the production side, where it sends predictive alerts and reports, as well as signals for anomaly detection. Another important aspect is the creation of decision-making rules for automation.

4. Application Layer

This top-of-the-line layer interacts directly with end users and business systems. Its functionality is quite complex. Basically, this layer provides interfaces for monitoring and controlling IoT devices remotely, displays visual analytics through dashboards and graphs, and triggers automatic actions based on the processed information. Its use is done through mobile applications, web panels and portals, but also through visualization and alerting tools. Its roles include remote device management, real-time status monitoring and integration with Enterprise applications. The IoT architecture has applications in various fields. In smart agriculture, this architecture automates, for example, irrigation schedules during certain periods, monitors soil conditions and analyzes crop health through real-time sensory readings. Another use is in car tracking, where it monitors the movement of vehicles, transports, and equipment using GPS telemetry and beacon signals. In smart grids, IoT architecture helps balance energy distribution, predicts consumption patterns, and reduces transmission losses. In the field of home automation, architecture controls lighting, door locks, appliances, and climate settings according to the user's habits. This emphasizes the need for proper construction. In terms of industrial automation, such a system can predict machine failures, schedule maintenance, and improve production accuracy, especially in factories.

Scalability is a great advantage of IoT architecture, as it allows for the integration of an increasing number of devices and sensors as requirements increase. Another important aspect is resource efficiency, which has been significantly improved. Thus, operations optimized through data-driven control contribute to reducing energy consumption and maintenance costs. In addition, data is collected in real time through sensor streams, which facilitates faster reactions thanks to instant visibility of ongoing processes.

Another improved aspect is interoperability, which allows communication between suppliers through open protocols, increasing connectivity in diverse environments. This is closely related to predictive analytics, which helps to anticipate equipment failures and workload fluctuations, using artificial intelligence models to prevent downtime.

On the other hand, there are also disadvantages in the Internet of Things. Parts of these disadvantages would be security vulnerabilities. Interconnected devices are exposed to cyberattacks, unauthorized access, and security breaches due to weak security layers. The management of the large volume of data and the existence of multiple endpoints make IoT solutions extremely vulnerable to various threats, such as DDoS attacks, device hijacking, unauthorized access, and data breaches. Also, the implementation of this IoT system comes with high upfront costs, as the installation of sensors, gateways, and communication infrastructure requires considerable investment.

Another source of problems stems from compatibility challenges. Due to system complexity and the varying standards of equipment vendors, communication protocols can create difficulties in integrating heterogeneous systems. In addition, the communication network often gives headaches. Signal and connectivity issues can disrupt data flow and disrupt real-time operations between remote deployments. Another major problem with these systems is complex maintenance. Thus, large-scale

IoT deployments require constant monitoring, regular updates, and specialized management tools [4].

Internet of Things devices, such as sensors, actuators, and other electronic components, play a critical role, as they are the primary source of data for measurement devices. With the expansion of the market for interconnected elements with automatic transmission, many manufacturers have emerged that have neglected cybersecurity aspects. As a result, inexpensive devices have been launched, but with security flaws that are difficult to fix, either through updates or other methods. This vulnerability of devices poses a serious security issue. Thus, ensuring the security of information and devices at the individual level becomes a priority, considering user privacy.

The authors of the study [5], identify three major trends in security. This approach is based on easy cryptography, non-clonable physical functions, and blockchain solutions. They point out that the main mechanism for securing IoT devices remains cryptography, but it needs to be adapted to today's challenges. Another promising method is the use of non-clonable physical functions (PUFs), which are highly compatible with electronic devices. Blockchain is also proving to be an interesting solution due to its high levels of security and the way it is implemented. Combining multiple authentication and encryption techniques is the future, offering significant advantages in terms of security, due to the high degree of authentication, integrity, and privacy in IoT. Finally, it is essential to protect both data and the people who use it.

Since 2005, when the first relevant architecture for the IoT domain took place [6], numerous IoT architectures have been proposed [7]. The reference model, however, is the one proposed by the International Telecommunications Union (ITU). Figure 3 shows the seven-tier IoT architecture as described by the ITU standard.

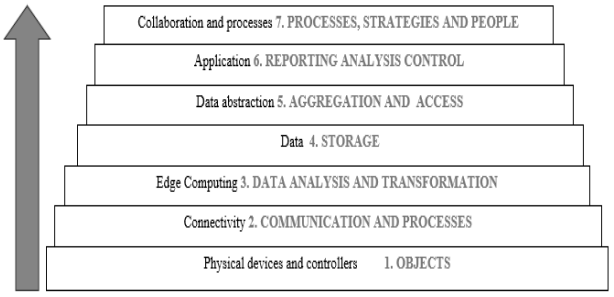


Fig. 3. IoT architecture structured on 7 levels with description (based on [8])

At the basic level (Physical devices and controllers), which manages the physical devices and collects the data. This is where the sensors that gather the information are located, as well as personal devices such as smartwatches and smartphones. The next level (Connectivity) is in charge for connecting and transmitting data to the higher levels. At this level, technologies and communication methods such as IR (infrared), Bluetooth, ZigBee, NB-IoT (Narrowband-IoT), 2G, 3G, 4G and 5G meet. Routers and base stations are also found here. The top level (Edge Computing) represents a processing point at the edge of the Internet. This level arose from the need to select the data to be transmitted further, having a filter that decides what information is relevant. Therefore, the presence of this level in the architecture is essential. The levels discussed so far have limited computing capacity. They focus on dynamic data, which is subjected to various operations and sent to other destinations. The data accumulation level and the data abstraction level are stages that no longer transform information, perform operations and no longer transmit actions on the data. At the Edge Computing level, computing power increases – higher performance devices are added – but this remains insufficient for the connectivity level. The main role of the data accumulation level is to store information from previous levels in databases. Here, the incoming data packets are filtered and stored in databases through relational tables.

The data abstraction layer focuses on retrieving and processing information, as well as making logical decisions based on it. This is where issues related to format incompatibility, semantics, and data security are solved. In addition, data is combined from various sources to create a more complete picture.

Next level, the Application level, is in charge of managing all the information coming from the data abstraction level, using different methods of extracting information through applications. This level coordinates all the previous ones, which must be designed correctly; otherwise, significant delays will occur between the data, affecting the response time of the final application. Although this level could also include the strategy, in most cases it is different, being more of a level of collaboration and processes. This is where executive models and reports are created, resulting from the analysis and accuracy of the data taken. The information provided by this level can be used at a strategic level to improve the IoT platform [9].

It is known that IoT architecture depends a lot on how devices exchange information with each other and with the cloud. In practice, there are three main models of communication:

1. Device-to-Device – here, devices connect directly, usually via Bluetooth or Zigbee. A classic example would be smart home devices that communicate locally.

2. Device-to-Gateway –devices connect to a gateway that handles the transfer of data to the cloud. It is a model widely used in factories or vehicles.

3. Device-to-Cloud – devices connect to remote servers via GSM or satellite networks. These are ideal for mobile or distributed assets. A well-developed IoT architecture often combines all three of the aforementioned models, thus providing flexibility and resilience. The evolution of IoT architecture The IoT architecture is in a continuous transformation. Older systems, from the beginning, focused on simple device-to-cloud connections. Today, there are distributed architectures that integrate artificial intelligence and edge analytics, providing lower latency and decision automation for each event.

Other authors [10] have come up with an interesting proposal: DTT Pipe. This system has the role of rigorously checking each IoT message before updating the Digital Twin – the Digital Twin (DT) – i.e. the digital copy of the analyzed system, which must always be up to date with the latest information, otherwise it risks leading to wrong decisions. DTT Pipe is an architecture that ensures the correct updating of the Digital Twin with IoT data. In ordinary systems, MQTT (a model that separates data producers from consumers) deals with the delivery of messages, but does not guarantee their authenticity or security.

This is where TDT Pipe comes in, an architecture that emphasizes security, controlling the entire path from publishing IoT telemetry to updating the Digital Twin status. It introduces a security filter between devices and DT. Each IoT message is cryptographically verified at the sequence level, thus also ensuring the plausibility of the values (e.g. temperatures, CO_2 levels). Incoming messages are classified into three categories: "Verified", "Suspicious" or "Untrusted", but only "Verified" messages are allowed to update the DT; "Suspicious" messages are quarantined.

The system generates a detailed history for each message, including information about where it came from. In addition, the architecture includes essential components such as the Device Registry, Security Gateway, and Audit Store. Tests show that the DTT Pipe works efficiently, with the ability to process thousands of messages per second.

Smart textiles are those materials that have embedded electronic components. This integration allows them to react to surrounding conditions. These types of textiles include sensors, microprocessors, and conductive fibers, bringing new functionality to traditional textiles. In recent decades, with the advancement of flexible electronics, the Internet of Things, and energy capture technologies, smart textiles have evolved rapidly. They are based on cutting-edge materials and technologies. For example, energy can be regenerated through movement or light, using thin batteries.

The development of smart textiles and wearable technology represents a significant step in uniting materials engineering, microelectronics, and IoT systems. By integrating miniaturized sensors, flexible circuits, and conductive fibers into traditional textiles, functional surfaces capable of detecting, processing, and transmitting data from the environment in real time are created. These advanced textile systems not only improve the functionality of common materials, but turn them into active platforms for biometric monitoring, thermal management, motion analysis, and digital interaction.

Integration of flexible electronics, miniaturized sensors, and IoT communication directly into textile structures is completely transforming the way wearable systems are designed. For engineers, these complex systems come with specific challenges such as interconnectedness, durability, electromagnetic compatibility, and energy management.

The future of smart textiles and wearable technology is full of exciting opportunities. Research and innovation continue to push the boundaries of what these technologies can achieve.

Future of IoT will be defined by software-based connectivity, private networks and the seamless integration of IT ecosystems. Scalability will not only depend on hardware and sensors, but also on how the entire architecture is efficiently orchestrated. There must be flexible, carrier-level infrastructures that can adapt quickly to emerging technologies. This flexible infrastructure must also provide stability in deployments on a global scale.

For example, ultra-thin sensors such as nanomaterials facilitate the creation of almost invisible sensors that bring new functionality without compromising comfort. Also, an interesting

direction is represented by self-healing materials. A relevant direction is emerging research is nano-technology. This direction includes fabrics capable of repairing minor damage autonomously, thus extending the life of wearable devices.

Medical and rehabilitation of textiles are evolving as wearable technology becomes increasingly sophisticated. Also, applications for remote patient monitoring and rehabilitation may expand. In addition, collaborations in luxury fashion are emerging. Top designers are beginning to integrate smart textiles into their haute couture collections, combining art with technology. Industrial safety is an ever-expanding field. In hazardous work environments, smart textiles can provide real-time monitoring of environmental conditions, protect workers and increase operational safety.

The integration of IoT in smart textiles should evolve beyond the current level, which is considered intelligent, and move towards autonomous systems. These systems should integrate cutting-edge technology, using artificial intelligence for advanced analytics. Textiles should develop the so-called "textile brains" customized for each situation and combining them should be done through sophisticated automation. Wearable textile sensors offer an extra added comfort.

On the other hand, the integration of electronic components into smart textiles contributes to environmental pollution, due to chemical reactions, degradation of solutions in manufacturing processes and contamination generated by the disposal of unnecessary components. Thus, textile sensors are extremely useful in applications such as posture monitoring, health analysis and in the field of sports. In addition, extraction and refining processes increase the temperature through the emission of air pollutants such as carbon dioxide and greenhouse gases such as nitrogen oxides. In conclusion, these aspects underline the need for the smart textile industry to adopt greener materials and more sustainable production methods [11].

8. CONCLUSIONS

The study analyzes the evolution and components of the Internet of Things (IoT) ecosystem, tracing its origins from military sensor networks to AI-integrated distributed infrastructures. It emphasizes the crucial role of electronic components like sensors and microcontrollers in data handling, noting their shift from simple data collectors to autonomous, self-maintaining systems. Emerging areas such as smart textiles, which integrate flexible electronics for wearable and medical applications, are discussed alongside challenges like sustainability and electromagnetic compatibility. The future of IoT is predicted to be driven by autonomy, flexible infrastructure, advanced security, and deep AI integration into smart devices and materials, with a focus on ambient computing and screenless interfaces. Also, integration and combination of this medium with clothes is presented.

Thus, the Internet of Things is moving towards hyperintelligent, decentralized networks, based on artificial intelligence and ultra-fast connectivity. Many objects (electronic components) in everyday life will process data locally and communicate in real time. A contemporary development direction is based on global, complex IoT ecosystems. In current times, electronic devices and the Internet of Things are becoming more and more known due to their potential, which has not yet been fully capitalized by business, academia or government. When electronic devices and IoT are used correctly, these industries can generate important financial and professional gains.

Development of smart textiles that are more flexible, sustainable, and commercially viable are being tested recently. The top trends defining the next wave of innovation includes smart fabrics. These smart textiles use conductive materials and microscopic dyes (known as chromic materials) that react to heat (thermochromic), light (photochromic), or electricity (electrochromic).

Additionally, a new generation of smart textiles that are more adaptable, sustainable, and profitable is under development. The leading trends that characterize the upcoming innovation wave are regarding conductive materials and tiny dyes, referred to as chromic materials, that respond to heat (thermochromic), light (photochromic), or electricity (electrochromic) and should be used in these intelligent fabrics.

ACKNOWLEDGMENT

This work was carried out through the Core Programme within the National Research Development and Innovation Plan 2022-2027, carried out with the support of MCID, project no. 6N/2023, PN 23 26 01 03, project title "Electroconductive materials based on multilayer metallization for thermoelectric systems, electro-

magnetic shielding and biomedical sensors integrated in IoT systems (3D-WearIoT)".

BIBLIOGRAPHY

[1] Haddaoui S. Seloua ,Chikhi S. Salim, Badreddine M. Miles. *The IoT Ecosystem: Components, Architecture, Communication Technologies, and Protocols*, 2022, Abdelhamid Ibn Badis, Algeria.

[2] Hassan, Q. F. *Internet of Things A to Z: Technologies and Applications*, 2018, New-York, USA.

[3] Lane J., Potok N. *Democratizing data: Our vision.* Harvard Data Science Review, **4**, April 2024, Cambridge, USA.

[4] Choudhary A. *Internet of Things: a comprehensive overview, architectures, applications, simulation tools, challenges and future directions. Discov Internet Things* 31, 2024, Germany.

[5] Zhang K.; Ni J.; Yang K.; Liang X.; Ren J.; Shen X. S. *Security and Privacy in Smart City Applications: Challenges and Solutions* , IEEE Communications Magazine, 55, 2017, New-York, USA.

[6] Aksu D., M. A. Aydin, *A survey of IoT architectural reference models*, 2019 16th International Multi-Conference on Systems, Signals & Devices (SSD), Istanbul, Turkey.

[7] Aldahr R. S., Thapa B., Maikoo K., Eduardo B., Fernández E.B., *Reference Architectures for the IoT: A Survey , Innovative Systems for Intelligent Health Informatics, Data Science, Health Informatics, Intelligent Systems, Smart Computing*, 2020 Langkawi, Malaysia.

[8] Tabbane S., *IoT Standards, Part I: IoT Technology and Architecture*, 2018, Bandung, Indonesia.

[9] Dragulinescu A.-M., *Internet of things. Dispozitive și tehnologii de comunicații*, Politehnica Press, Bucharest, Romania, 2024.

[10] Vicenzo de A. , *TDT-Pipe: A Security-Aware Architecture for Trustworthy IoT Digital Twins*, Future Internet, 18, 458, , 2026, Reggio Calabria, Italy.

[11] Ahmed A., Hasan E.U., Hasseni S.-E.-I. , *Smart and Sustainable: A Global Review of Smart Textiles*, IoT Integration, and Human-Centric Design, Sensors **25 (3)**, 2025, Bozen-Bolzano, Italy.

About the author

Scientific Researcher, PhD Engineer **Octavian-Adrian TABĂRĂ**
National Research and Development Institute for Textiles and Leather, Bucharest, Romania

The author holds a PhD degree obtained in 2013 at the Polytechnic University of Bucharest on the subject of magnetic hysteresis modeling. His areas of interest include numerical modeling, programming, development of new and innovative programs in various programming languages. Given the experience in the practical domain, gained after completing his studies, the fields of interest have diversified and currently the author focuses on a better compatibility between the theoretical and experimental parts in the field of textiles. The author has written several scientific papers, in various fields and in national and international journals, being also the author of a book that was launched at the Gaudeamus Book Fair in 2018.