PAST KNOWLEDGE PEOPLE

ISSN: 2640-4133

Review Article

Advances in Bioengineering & Biomedical Science Research

Clinical laboratory From Automation to the Internet of Things (IoT)

Angel San Miguel Hernández*, Julia San Miguel Rodríguez

Department of Clinical Analysis Service and Research Unit, Rio Hortega University Hospital. Valladolid, Spain.

Professor at the International University of La Rioja (UNIR).

***Corresponding author**
Angel San Miguel Hernández, Department of Clinical Analysis Service and Research Unit, Rio Hortega University Hospital, C/San Antonio de Padua 1, 1º Dcha 47003, Valladolid, Spain

Submitted: 10 May 2021; **Accepted:** 15 May 2021; **Published:** 25 May 2021

Citation: *Angel San Miguel Hernández, Julia San Miguel Rodríguez (2021) Clinical laboratory From Automation to the Internet of Things (IoT). Adv Bioeng Biomed Sci Res 4(2): 38-53.*

Abstract

Internet of things (IoT), is a network of physical objects, vehicles, machines, appliances, etc. that uses sensors and APIs to connect and exchange data over the internet. IoT relies on a comprehensive set of technologies, such as application programming interfaces (APIs) that connect devices to the internet. Other key IoT technologies are Big Data management tools, predictive analytics, artificial intelligence and machine learning, the cloud, and radio frequency identification, among many others. Cloud-based IoT platforms and architecture connect the real and virtual worlds. They help companies manage the security and connectivity of IoT devices, as well as collect device data, link devices with backend systems, ensure IoT interoperability, and build and operate IoT applications. Smart devices generate an enormous amount of IoT data that must be analyzed and harnessed in real time. Predictive analytics and Big Data appear here. Machine learning is also used to add context to data and generate actions without human intervention. The IoT related to the clinical laboratory, will revolutionize the concept of this, since it will be easier to connect with other laboratories more efficiently, with clinicians and with patients. And the latter will then be at the center of the Health System.

Keywords: Internet of Thing, IoT, Automation, Clinical Laboratory

Introduction

Laboratory automation uses robotics, artificial intelligence (AI), and other technologies to automate manual and large-sample tasks in clinical and research laboratories. Automation can accelerate turnaround time and discoveries in both clinical and research labs, including labs in hospitals, pharmaceutical and biotech companies, universities, and other research institutions [1-7]. Laboratory robotics and automation are equipped with a range of hardware and software, sometimes with special capabilities for computer vision or other types of AI. Automation in the laboratory medicine of the future until now, the challenges of today's clinical laboratory have been to reduce errors, increase service levels, optimize resources and achieve cost containment. In order to improve the production process, unified laboratories or core labs are implemented with two automation models: the fully automated laboratory and the modular automated laboratory. Today that automation expands practices. Starting with the basic automation components within the clinical laboratory such as instrument automation, LIS/LIMS and pre and early analytical automation, there are different laboratory automation strategies, which are listed in Table 1 [1, 5, 8]. Automation relies especially on robotics, which can change the working method of specialists in a laboratory. In addition, the sophistication of specialized machines will multiply results in an ever easier and cheaper way. The new practices are specified in what is summarized in table 2 [1, 9].

Table 1: Different strategies in the automation of the clinical laboratory

-LIS / LIMS systems.
They are complex platforms that direct the laboratory workflow.
-Open automation.
Solutions are vendor-designed and can be connected to any instrument in the lab.
-Reduce errors and more performance.
There is a growing demand for testing and testing reimbursement, forcing labs to optimize performance.

Table 2. New practices in the clinical laboratory Computer vision and other types of AI speed up work in the laboratory

-In the automatic processing of samples.
Machines are becoming faster and more efficient in chemical and biological processes, and this allows reducing waiting times for results.

- Most commonly used equipment.
Both biochemistry, hematology and enzyme immunoassay analyzers are widely used equipment in the automation of a clinical laboratory.

- Have personalized workflows.
Robotics will become increasingly easy, intuitive and flexible, until specialists can adapt it to their way of operating.

-More fields from the lab.
Clinical chemistry and hematology were the first to be automated, followed by enzyme immunoassays, molecular diagnosis, and anatomical pathology.

- Automated liquid handling.
The instruments reduce the time required to perform repetitive volume pipetting tasks at high process speeds. -Integral management of sample tubes. Automation enables the life of a tube to be tracked, thus managing pre- and post-analytical processes more efficiently.

-Objectives and resources.
Before implementing a solution, laboratory managers must know what they want to achieve with the automation and resources required. This is the only way to achieve a solution that will prepare your laboratory for the future.

Thus, laboratory automation frees professionals from time-consuming manual tasks so they can focus on new and more important tasks. Patients can quickly receive their diagnoses and new drugs can be tried quickly, leading to state-of-the-art treatments. In this laboratory of the future, artificial intelligence takes automation to the next level.

In hospitals and healthcare systems, clinical laboratory automation enables high precision and fast turnaround time for diagnostic tests. Also in pharmaceutical research and development, laboratory automation helps to perform a large number of experiments in a short time. And technologies drive laboratory automation solutions ranging from robotic arms with computer vision to high-performance image analysis. Therefore, whether it is running a simple blood test or analyzing the effects of a treatment on cell culture, some of the most important answers in health come from the laboratory.

A laboratory evolves with high precision, fast speeds, and high throughput. The more efficiently a laboratory works, the faster tests can be performed to reach diagnoses for clinicians, thus accelerating the delivery of medical care. Laboratory automation involves a set of technologies that automate high-volume, manual tasks in clinical or research laboratories. In a large number of cases, these technologies involve laboratory robotics and AI, including machine learning, deep learning, and computer vision. Laboratory robotics and automation can be applied to a variety of work processes and equipment, from reference instruments to standalone systems to microscopes. Depending on how they are used, laboratory automation systems can be single-function or combine many different functions [8].

Automation in a clinical laboratory is primarily focused on ensuring accuracy, while speeding up the time and efficiency of diagnostic tests. Clinical laboratories usually work around the clock. It is important that the technicians of these laboratories manage the large number of tests they receive from one or more hospitals or clinics. The latest clinical laboratory automation solutions use computer vision to read barcodes, identify samples, and help robotic arms to perform precise movements. Clinical labs are also exploring the use of machine learning in areas such as digital pathology, which requires a high degree of computing performance on edge servers.

Robots in the reagent liquid handling chains, sequencers, high-content screening, etc., are among the laboratory automation systems that also help accelerate pharmaceutical research and development. Professionals can perform a large number of tests and / or experiments, which can lead to the discovery of new drugs, cancer therapies, and other treatments. Machine learning and deep learning are particularly valuable in research labs, with algorithms that speed up high-content screening and other imaging workloads [1, 8].

Benefits of Automation

Automating manual processes in the laboratory leads to many benefits, especially the time it saves, which are summarized in Table 3. But even more important is when tasks are completed faster while maintaining accuracy. For example, when researchers can rapidly run a million compounds against a target drug, they can discover a breakthrough treatment at blazing fast speed [10].

Table 3: Advantages in the automation of manual processes in the clinical laboratory

-Reduction of errors.
By design, laboratory automation reduces the possibility of human error by eliminating manual labor from the process. And it supports reproducibility and consistency in testing.
-Fast delivery time of results.
Automated systems can perform high-throughput screening and other experiments at a rate not possible for humans, while maintaining accuracy (2)
-Strategic use of human personnel.
Lab professionals can focus on their most important capabilities and focus on strategic tasks.
-Cost reduction.
Laboratory automation systems can help reduce costs by reducing the volumes of reagent required and minimizing waste. -Safety in the workplace. By minimizing the need for human intervention, laboratory automation can help technicians limit exposure to pathogens and harmful chemicals or injuries caused by repetitive motion.

Technologies for Comprehensive Automation in the Laboratory Internet of Things (IoT)

Laboratory Automation Technologies ranging from robotic arms to image processing, different technologies drive the latest laboratory automation solutions. The multitude of computing technologies offers instrument manufacturers a wide range of computing options that meet power and performance requirements, along with software-enabled capabilities for computer vision and other types of AI. Additionally, servers and storage built on different technologies provide a solid foundation for data management throughout the lab. This is compatible with the principles of FAIR data (as open as possible, as closed as necessary), making the data findable, accessible, interoperable and reusable in automated systems without human intervention [11-13].

-Current processors offer the right level of performance and energy consumption necessary to automate laboratory processes. This is ideal for sample handling and recovery, sorting, centrifugation, and other pre- and post-analytical functions.

- Scalable processors offer high performance for edge servers in the lab, especially useful for high content screening (HCS) and other types of images.

-Vision Processing Units (VPUs) are designed for perimeter computer vision. These low-power VPUs allow barcode reading, robotic arm movement, sample analysis, and much more Persistent memory and solid state drives support large in-memory applications, ideal for imaging and AI workloads in lab automation.

- For developers, it offers software libraries and optimizations for popular frameworks to boost performance in architecture.

-Support for the latest Wi-Fi and 5G standards, which simplify the process of connecting instruments in the laboratory. High-speed connectivity enables remote control, real-time monitoring, and other edge-to-cloud use cases.

With the growing growth of the Internet of Things (IoT) in Healthcare and other sectors, the Healthcare industry is being revolutionized by redefining the interaction between devices and people. IoT helps build an integrated system that ensures that patients receive better care, with reduced costs and better treatment results [14, 15].

The Internet of Things (IoT) is the new trend of devices on the market. This technology is being developed by multiple companies around the world to solve specific problems of people. However, there are currently cases of security flaws in IoT devices, in this case in hospitals. The different security methods that companies have implemented in their solutions and products, from wired and wireless topology designs, to strict perimeter security of the different layers, which work in conjunction with secure programming and recommendations for the end user, make proper use of it [16-19].

The objective is to implement in our IoT system, an extra layer of computer security without depending on the supplying company, which has embedded it in their product. This layer makes it difficult for the attacker to manipulate our equipment at their convenience or to exploit a known failure in a device that could harm the life, health and integrity of the patient.

Benefits of IoT in Health

Effective Patient Management

With the wide spread of device connectivity, healthcare organizations have access to real-time information about patients. This helps you make informed decisions about what treatment to seek and the right time to seek it. Also with the availability of continuous monitoring, diseases can be identified at an early stage and treatment can be started before the patient gets worse. Therefore, the spectrum of care in preventive medicine is broadened.

Better Patient Care

This means better diagnostic precision, more timely actions for clinicians, and better results from IoT treatment. The patient's needs are served efficiently and effectively. This improves patient confidence and helps maintain responsibility for the service. With this, we achieve that the patient becomes the center of the System [20, 21].

Decrease in Service Expenses

With the recent growth in real-time patient monitoring and device drug delivery, unnecessary doctor visits are reduced, which also reduces spending for public and private healthcare organizations. Added to this, in direct patient care facilities where advanced systems are available, for hospitals and Health Centers, there is the possibility of reducing hospital admissions. And thus, the System becomes more sustainable [22, 23].

IoT challenges

IoT offers many positive aspects for the Health industry, such as:

Data Security

Although IoT is transforming the healthcare industry, there are also a number of challenges given that patient data is sensitive and has the highest level of security. When such information is shared inappropriately, it can cause a bad reputation and serious harm. With the increase in data volume, there are more threats from cyberattacks and more appropriate measures are required. Therefore, cybersecurity must be promoted in healthcare organizations.

Dependence on Infrastructure

The IT infrastructure of the industry will experience stress with the increase in the exchange of health data that expands. There may be multiple devices in use adding to the risk factor. And it will be necessary to adapt the information and communication technology (ICT) infrastructure to mobility and data exchange. Because of this, the IoT will change Healthcare, forever. Ultimately, this makes the popularity of the IoT grow in the healthcare industry with the pros outweighing the cons. But, extra precautions must be taken when using IoT, providing an extra level of security and using IoT experts on the team.

Enabling the Laboratory of the Future in the IoT

The IoT has already begun to break down millions of data and enable a new level of automation. Microscopic images are processed in real time. Test and experiment results can be analyzed and shared with laboratories around the world. The data from the probes can be applied to AI algorithms, to inform predictive maintenance, which in turn avoids instrument downtime [13, 14].
Figure 1 shows the concept of IoT applied to the clinical laboratory.

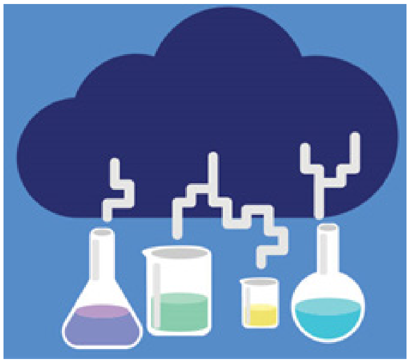

Figure 1: Schematic concept of the IoT applied to the clinical laboratory

Fast networking, storage and processing technologies will continue to increase the efficiency of the laboratory of the future.

As clinical laboratories, researchers, and pharmaceutical companies become more connected and automated, the foundation of technology that efficiently moves, stores, and processes data will be provided. Whether analytical testing in the cloud or robotic arms at the edge, the technologies enable intelligence at every step in the automated lab. Therefore, connecting devices, digitizing processes, using data from sensors, is what different companies are advised to work with an IoT laboratory and with a cloud platform.

No one is going to escape the IoT in the next few years and the important thing is to lose your fear and get started. Since many times things are less complex than you think. Several professionals can build a technical infrastructure. Some memory capacity, databases, analysis systems and modern development platforms, since no more is needed to start the process, to achieve a basic IoT framework. The next step would be to identify which employees already have experience or knowledge on the subject and look for the most relevant use cases. So it would be good if more and more services emerged for the different areas of work, since it is essential to get their acceptance.

The factors that must be met for the IoT implementation to be effective. The most important thing is that the management supports the IoT. You must make the strategic decision that sensor-assisted products and processes are useful for the company and, therefore, invest in it. Subsequently, there must be trained employees from the product R&D areas to address the issue and promote it in the company. At the beginning, with starting a very specific first project and developing the activities in the framework of an IoT laboratory successively. Then, it is important to communicate and discuss experiences and positive results in the company. Ideas for IoT-based innovations are growing upward across different departments and business areas. Ultimately, the IT department for the development and management of IoT workloads and IoT-based products must equip the company. This requires tools for visualization, special memory and computational capacity for log and sensor data, databases and analysis systems for real-time processing. In addition, systems must be scalable, as it cannot be predicted to what extent services will increase. Therefore, cloud platforms, such as SAP HANA Cloud Platform, play an important role for the IT back end in the implementation of IoT projects. This is because cloud-based platforms have the advantage that large up-front investments are not required and the team can get down to business and be productive.

A company of whatever type, laboratory or otherwise, cannot avoid working in an interdisciplinary way. Experts and engineers with the expertise from technical product development should sit at the same table alongside software developers and IT architects. It is the only way to develop truly innovative and customer-oriented IoT products and services. In the beginning, the learning curve is very steep. Currently, many companies are beginning to implement IoT technology. Technologies, be it sensors or cloud-based analytics platforms, represent new territory for many users. IT service providers can help in the early phases, of course, also the internal IT team, as long as they already have experience and knowledge on the topic of IoT. IoT

Technologies and Automation Can Revolutionize Lab Practice

Adoption of IoT in labs marks a major technology disruption. Its implementation will replace an old and less inefficient system with one that maximizes the time of the instruments and the physician to their maximum potential, stimulating new scientific efficiency and, therefore, innovation [24-26].

There is a tendency for some to continue old practices simply because it is what they have become used to. The current system is stalling progress as it does not take full advantage of 21st century technological advances or maximize research equipment, time, or potential. We must take full advantage of the opportunities provided to facilitate faster and more accurate investigation.

In the old system, professionals had to manually mediate and record the data flow. And these professionals would have to be physically available in the laboratory to perform tests or experiments and conduct their studies according to their schedule, working when it was convenient for the professional, rather than arranging for the experiment to run at the optimal time. Typically, you are not connected to the internet and you would have to manually enter data in a digital format from a fragmented work environment. With the recent introduction of these concepts, such as smart homes and smart cities, it is not surprising that this same concept is now being applied to create smart laboratories. Now imagine a laboratory that maximizes team capabilities, work time, research, and effort. Through new innovations that allow the connection of existing instruments to the cloud or a local server, combined with the introduction of laboratory automation and drones, the laboratories of the future will be unified, flexible and accessible from anywhere. The new systems available will use Internet connectivity to monitor instruments, create alerts and store data. This will allow researchers to operate instruments remotely and receive alerts in the event of a machine malfunction, increasing efficiency while accelerating scientific innovation and discovery. A smart lab connected to the IoT can be tailored to meet the specific requirements of any lab. It is a flexible and adaptable innovation that can accommodate all varieties of researchers.

An intelligent laboratory can monitor inventories of laboratory items, monitor environments, such as controlling temperatures in incubators or freezers, and can facilitate communication between professionals. It will allow professionals to view data on machine usage, allowing them to make important decisions regarding usability and productivity [27-30].

Therefore, the opportunities are endless. The sensors can be installed in laboratories to track the progress of different chemical reactions and this information can be transmitted directly from the sensors to an Electronic Lab Notebook, software that allows scientists to document their research data in a digital format online. The benefits of having an electronic lab notebook and a lab automation system are undeniable as it allows a scientist to manage their research data on a unified platform while monitoring the output of internet connected devices. Many of the perceived costs with respect to the smart laboratory are related to the financial cost of implementing connected systems in existing laboratories. Researchers may hesitate to accept the new changes for fear of spending money on a product that will be further updated in the coming years. Upgrading only half the equipment also creates problems, as it fails to achieve one of the key goals of smart labs, which is to unify the lab [31-34].

However, there are alternatives, one of the ways is that a lab could gradually implement IoT at no upfront cost and implement internet connectivity on existing machines or have a device that receives the data from their machine. This is a Lab Execution System, which is a cheaper alternative and can collect data from the instrument in real time and at the same time manage your devices remotely. Investing in such a system would allow the gradual implementation of IoT in the laboratory, at which point one could evaluate what products are available, taking into account their safety standards and the extent to which that laboratory would have a specific requirement.

When we think of IoT, security is always an issue. Some professionals are hesitant to adopt IoT technologies in their existing system due to mistrust of security features when it comes to the Internet, especially when using the cloud [35, 36].

However, it's important to note that all of this innovation doesn't mean you need to store data in the cloud, which is a key source of the reluctance to adopt IoT-enabled devices. Some products allow you to choose whether you want to store your data in the cloud or on a local server, ensuring that you have the option of putting your data in the cloud or protecting your data on a local server behind your firewalls.

Security is an issue that certainly needs to be considered when implementing IoT in a lab, but it should not be an issue that dissuades people from the concept of smart labs. It should make scientists more careful when choosing a product. To combat the security threats posed, a laboratory needs to implement strong and reliable security configurations that ensure protection of intellectual property. Additionally, data can be protected by implementing a secure and reliable infrastructure combined with good laboratory and security practices. If researchers adopt good security practices, the risk is significantly reduced.

One of the most important opportunities that smart labs allow is the improvement of the quality and speed of the research produced. Intelligent laboratory automation will significantly improve data accuracy and reduce data entry error. Implementing IoT in the lab will allow machines to collect and measure data, transmitting the data to a central storage repository, allowing materials to be accurately collected and recorded.

Laboratory automation can also improve laboratory efficiency and encourage good practices. IoT is a technological innovation that presents many exciting opportunities for the area of science and discovery. This network of humans and physical devices allows researchers to solve problems that would normally take hours or days to solve, paving the way for cheaper experiments and faster results. Scientists can use this obtained connectivity to unify laboratory equipment, ensuring that research is not limited to one individual's schedule.

Some have called the introduction of the IoT the fourth industrial revolution, and to a greater extent, this is the case, when considering the improved efficiency of smart labs. The flexibility and accessibility provided by Internet-enabled devices will drive innovation at a faster pace, leaving traditional labs in the past.

How the IoT is affecting laboratory equipment, this is a paradigm shift in our way of thinking about laboratory equipment. It is possible that entry into the lab could be delayed, but that will quickly become an unfeasible option, as more manufacturers incorporate IoT into their instruments. A much wiser use is to adopt the IoT, but with a controlled process to reduce the risk of security breaches. One of the commonly cited characteristics is that it focuses on machine-to-machine (M2M) communication. Beyond that, it generally refers to any device, virtual or physical, that can be connected, either directly or indirectly, to the Internet. It is projected that by the year 2023, the IoT will consist of approximately 2.98 x 1010 discrete devices, far outnumbering human internet users (38-40).

Unfortunately, while the big picture of the IoT can be presented quite simply, when you are in the middle of deciding how to implement and configure it, things can get quite messy, at least during this period of its development.

Approaches to IoT

There are several approaches to implementing IoT devices. Currently, the most widely used is to implement a standard TCP / IP stack in the IoT unit and have it communicate like any other network device. The advantage of this is that it uses a technology familiar to most IT groups. The downside is that the cost of integrating the hardware and software to make this possible increases the cost of the individual sensor devices. However, it does allow handshakes between devices, so you can confirm that a message was received [41, 42].

An alternative approach is to use several inexpensive sensors incorporating a much less expensive simplified or lightweight communication protocol. This uses an extensible open source structure that comprises private data fields and is validated with a simple checksum, known as Chirps. For devices that report small amounts of data, using Chirps to transmit these reads significantly reduces the amount of overhead on the packet structure. The trade-off is that no confirmation on receipt of these Chirps is transmitted. The philosophy is that due to the low cost of the sensors, multiple redundant sensors can be distributed, so that if a reading is lost, it has no impact on operations [43, 44].

Whichever approach is taken, it still needs to receive the data. This requirement can be addressed in two ways. The classic approach would be to incorporate code into your applications, such as a Laboratory Information Management System (LIMS) for an analytical laboratory or a Supervisory Control and Data Acquisition (SCADA) for a process control system. However, this approach requires custom system modifications for each sensor you add. In most situations, it is much more pragmatic to use a Web of Things gateway, which could consist of a software layer of middleware on your network or a module of physical hardware. The purpose of this gate is to aggregate the data from IoT devices, filter out unnecessary information, transform it into a format that instruments and applications in your labs can understand and deliver. Vendors are developing a series of proprietary gateways. However, the basic operation of these gateways can be illustrated with the open gateway for the Internet of Things being developed by Mozilla.

The IoT promises a major paradigm shift in the way we work and think of our teams. The magnitude of this change is suggested by referring to these devices as enchanted objects. The inference is that they are more intuitive to use and do not require you to learn a new set of commands and procedures for each device. While many benefits will be common to all laboratories, some may be specific to the specific type of laboratory being administered [45, 46].

If the range of analytical, process control, clinical / hospital and other laboratories is considered. The applications that can be included are listed in table 4.

Table 4: Applications that analytical-clinical laboratories can include in the control of clinical/hospital processes.

-Monitor reagent inventories and automatic reordering.

-Monitoring of controlled environments, such as server rooms or reagent storage areas, to detect excessive or insufficient temperature conditions.

-Monitoring equipment for regulatory or operational compliance. This could range from monitoring incubators or freezers to ensuring they stay within their optimal temperature range.

-Security monitoring and remote communication with employees.

-Monitor the temperatures of the samples, whether collected internally or externally, to ensure that there are no deviations outside the regulatory storage temperature range. Possibly even capturing the actual sample collection point. Other laboratories will have different requirements, with varying degrees of overlap, among which are:

-Monitoring of the identity, location and status of patients.

-Allow observation notes and inputs as well as treatment orders via smart pens.

-Data capture from independent instruments. -Monitoring of the status and location of professionals in different situations through portable devices.

Right now, it is only getting started with regard to the impact of IoT-enabled devices. In the future, there will be an ever-expanding range of uses, limited only by imagination.

As with most technologies, there are also drawbacks for IoT devices. Some of these problems are due to errors in the design or programming of the device. Other questions refer to the privacy and confidentiality of the data collected [47]. But this is much less compared to active attacks on the IoT. So far, the main goal is to subvert the IoT for criminal purposes. Some of the biggest denial of service attacks found so far have been launched on the use of Internet security cameras and other IoT devices. This is not the only risk, as once a single device's security is penetrated, it can be exploited to launch attacks against other components on the network. With some IoT devices, there may be little physical risk, but if the IoT devices in question control valves and heaters in a chemical production process, they could be used to generate an explosion [49-52].

Unfortunately, as we are basically on the edge of IoT, many of today's IoT devices weren't designed with security in mind. Many already installed devices can be easily tampered with and the cause of the resulting problems can be difficult to detect. Part of this is that manufacturers, whose engineers are not used to thinking in terms of security, quickly launch products to market without realizing how they have increased the potential attack surface of the overall network. To some extent, this is understandable, as the design requirements for security are not the same as those for security. In some cases, it is impossible to optimize both, so you must determine the best balance to minimize overall risk [53, 54].

Several groups are applying new security practices for both the design and implementation of IoT devices. There are a number of steps that as a laboratory professional, you can take to minimize this risk, ideally working closely with your organization's Information Technology (IT) group. Some of these steps are relatively simple, but someone must take responsibility for making sure they are carried out, these are summarized in Table 5.

Table 5: Steps to be followed by the personnel for the best security measures that are carried out to minimize the risk.

-Change the password on all IoT devices before installation. If the manufacturer has a fixed password that cannot be changed, choose a different provider.
-Make sure all unused ports and protocols on the device are disabled.
-Ideally, all data transfers must be encrypted, and each device must use a different encryption key, even if IT must configure a public key infrastructure (PKI) from scratch.
-When possible, buy equipment that supports firmware updates over the air (OTA).
-Do not buy equipment with known security problems, even if you must lose some functions. Money talks and can drive security development.
-Security practices are different for IoT systems and traditional networks, so IT staff may not be familiar with the differences. And ensure proper procedures are followed
-Ensure that a compliance monitoring program is established for IoT, to ensure its security is met

An IoT implementation can revolutionize your lab operations, but it has risks. Particularly as manufacturers and IT support teams explore this new paradigm, it is not unlikely that some of the IoT devices already within your organization have been compromised, so you need to coordinate with IT to make sure. that all devices have been locked, both to ensure the security of your operations and to eliminate possible legal liabilities. With a proactive approach, the IoT allows you to redesign many processes, improving both data quality and productivity [54, 55].

In the manufacturing industry, IoT is transformed into the Industrial Internet of Things (IIoT), also known as the Industrial Internet or Industry 4.0. The IIoT uses machine-to-machine (M2M) technology to support everything from remote monitoring and telemetry to predictive maintenance.

Uses of IoT and its Applications

An overview of the benefits, possible use cases, open challenges of cloud computing and fog in the context of IoT will be made. Since both approaches have different benefits and will see a broader adaptation. A suitable solution is for both paradigms to combine to achieve seamless integration of cloud and fog resources in a common pool of IoT resources.

The basic concept of IoT is shown in Figure 2.

Future developments will include mechanisms for fog-cloud interaction, such as automatic resource provisioning, replication, and migration, which are essential to meet the resilience and reliability requirements of the IoT [56, 57].

Figure 2: Outline of the IoT concept

The value-added service will need to be defined only once and will be automatically provisioned and relocated on demand, to a suitable compute node. Existing services could be combined to create innovative new services. Advances in security and privacy will help keep sensitive data private across all processing nodes from different vendors. Despite the remaining challenges, cloud and fog computing are indispensable tools for realizing a more seamless IoT ecosystem [57, 59].

The two main paradigms for the treatment of large amounts of data. The concept of big data is based on a posteriori analysis of the data in batches, while the big stream rewards a real-time analysis, in addition to being able to act more quickly in case of detecting any inconsistencies in the data series (60.61).

Unlike classic wireless sensor networks (WSN) that generally only serve a single application, one of the main benefits of the shift to

IoT lies in the common use of the same hardware or device by heterogeneous applications. In addition, the IoT revolution is not derived only from the number of connected devices, but from the solutions and services offered on the data. The basic requirements of such services can be briefly summarized as follows: non-volatile storage of historical data, data processing, and efficient near real-time distribution of data. In general, an IoT environment is divided into three different layers or environments, which are cloud (cloud), fog (fog) and edge (edge), as we observe collected and summarized in figure 3.

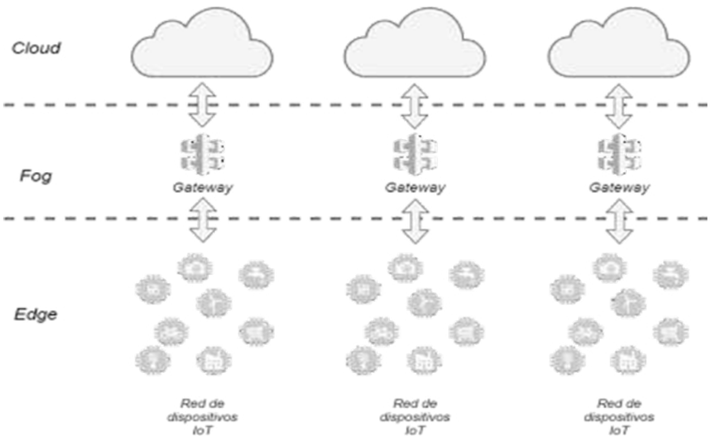

Figure 3: Different layer hierarchies involved in IoT scenarios: The fog layer functions as an extension of the cloud to the edge of the network, where it can support data collection, processing, and distribution. Cloud computing (cloud). Fog computing, Edge computing (26-30).

Traditionally all the computing power resided in the cloud, the rest of the layers only had the commitment to generate and transmit the data. Cloud computing offers convenient, ubiquitous, and on-demand access to configurable computing resources, which can be accessed via the Internet and generally reside in third-party data centers. Along with these resources, cloud service providers offer fast and configurable networks for data distribution, as well as reliable, non-volatile and replicated storage. Due to its flexibility, reliability, and usage-based payment model, cloud computing is well positioned to meet specific requirements in the context of IoT [30].

Although this architecture currently works well, it is not suitable for latency-sensitive applications, as data centers in the cloud are not located, neither with connected objects, nor with consumers of value-added services. From a network topology standpoint, cloud data centers are several leaps away from producers and consumers of IoT data. Physical distance causes additional latencies that may not be acceptable for applications sensitive to it, such as device health reporting tasks. Therefore, rather than forcing all IoT communications through a cloud broker, a push has been given to promote data storage, processing and distribution closer to the edge of the network, towards producers and consumers of data [32, 35].

One of the main challenges is that commonly used devices, such as sensor nodes, smartphones, and wearable technologies, are generally battery-powered, making complex storage or processing of a large amount of data unfeasible. The connected objects belonging to a network can also often be too limited to perform those tasks as reliably and quickly as necessary. Devices with restrictive features can save energy by transferring their data to a cloud-based platform where it will be distributed to multiple relevant applications and services, which will process the data accordingly. With the passage of time, IoT devices are increasingly connected to the internet and becoming more and more powerful, but in general they are not capable of large enough processing. Therefore, in recent years, computing power has been placed in the fog (Fog Computing), which can be seen as an extension of cloud computing, but which allows services closer to the edge of the network, where cloud and fog computing paradigms share many characteristics [40, 44].

Cloud computing is primarily targeting applications and services that would not be feasible in the cloud. One reason would be to eliminate bandwidth bottlenecks and improve latency for the most common tasks in the context of IoT. To achieve this, fog computing uses the local processing power available today, such as in network hardware or local gateway nodes (gateways), mobile phones, or additional hardware that would have to be deployed in the future between IoT devices and the cloud.
Also in recent years, new developments of IoT devices have appeared with very powerful computing characteristics, capable of performing processing on themselves and obtaining results at the same edge layer.

Edge computing primarily offers two enhancements. One is that the results are obtained on the same device, so in the case of notifying the user it is immediate, and the other is that it is due to the reduction of traffic to the upper layers, since with the sending of aggregates or the results themselves may be sufficient. For cloud and fog-based computing approaches in the context of IoT, different advantages and challenges are presented and specific use cases of IoT that benefit from cloud and fog computing, respectively, are described. The primary concern when looking at cloud and fog computing is the actual role these technologies are expected to play in IoT systems.

The basic architecture reference model, it has three layers:
-Device layer,
-Connectivity layer and
-Application layer

Generally, cloud and fog technology will be used to realize the connectivity layer by transmitting device data and enabling value-added services at the application layer.

The functions that are expected to be obtained from both paradigms for an IoT system are [27-29]:

Data Distribution

IoT environments will generate huge amounts of data that can be useful in many ways. The first requirement is to provide ubiquitous, real-time access to all data by distributing it from data sources such as sensors, wearable devices, and smartphones, to consumers, such as actuators, value-added services, and applications. The great diversity in hardware and software highlights the need for a unified messaging middleware that interconnects data sources to consumers by providing uniform and standardized application programming interfaces (APIs).

Scalable Storage

The value of the vast amount of data available in IoT may not be directly apparent in the collection, but the data can provide very valuable insights in the future. Therefore, for many use cases, scalable storage and ubiquitous access to historical data will be a valuable feature.

Processing Services

Big data analytics and processing have become increasingly relevant to the IoT ecosystem. Raw IoT data alone is not very valuable, but value-added services can apply some kind of analysis, such as temporal and spatial aggregation and correlation. In addition to these basic services, there are other additional qualities at a high level imposed by the specific use case of IoT.

Flexible Self-Organization

The IoT must be self-organizing. While devices must be uniquely identifiable, new data producers can join or leave the system at any time, so it must allow discovery of relevant data sources and services from a heterogeneous and ever-changing mix. In addition, the system must be able to adapt automatically to the changing needs of data consumers.

Reliability

Depending on the use, strict requirements for reliability and quality of service must be adhered to, such as low latency and reliable end-to-end data delivery.

Scalability

Due to the large number of connected devices, as well as the expected data consumers, the system must be scalable. In other words, the system must provide adequate basic services regardless of the number of connected devices, services and consumers.

Confidentiality and Data Security

Device data or derived ideas may be confidential, may also not be shared with certain entities, or may not be transferred or stored in other legal areas. The IoT system must support those requirements and ensure that restricted entities do not access the data. The aforementioned requirements motivate the use of cloud and fog computing over an IoT architecture.

Cloud computing refers to both a subset of applications available through services over the Internet and the underlying hardware and software systems in data centers that enable those services. And it is divided into infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

IaaS

It provides processing, storage, network communication, and other computing resources that enable the consumer to implement and run software, including operating systems and applications. The consumer has control over operating systems, storage, deployed applications, and possibly limited control over some network components.

PaaS

Provides the ability to deploy consumer-built or purchased infrastructure and applications. The consumer has no control over the underlying infrastructure, such as network, servers, operating systems, or storage, but only manages the deployed applications.

SaaS

Provides the ability to use the provider’s applications, which run on the cloud infrastructure. These applications are accessed from client devices through the appropriate interfaces. The consumer does not manage or control the underlying cloud infrastructure or individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Cloud computing can help the development of IoT systems to meet most of the requirements. In fact, the approach to send data from an IoT device to a cloud-based service for messaging and processing is widely adopted by developers.

Additionally, solutions for many common tasks are already offered as hosted services from cloud providers, including storage, messaging, and processing. For example, there are PaaS providers specifically for IoT systems, such as Amazon Web Services (AWS) IoT, that offer a gateway for IoT messaging needs, a rules engine for data processing, and a server. Database (DynamoDB) for storage and queries.

Other vendors, such as Microsoft, IBM, and Xively, also offer very similar services. There are also SaaS providers in the IoT ecosystem that offer purpose-built services such as smart heating or building automation. Like companies, which market smart thermostats for domestic users with the aim of reducing the cost of heating. Most IoT service providers use a three-tier architecture. Many end devices characterize the typical cloud-based IoT solution; these produce data that is typically used by gateway nodes to communicate with a wide area network, typically the Internet. Storage, messaging and processing, which are crucial for IoT applications. The queues and messages layer is often used in an event-based publish / subscribe system in the cloud-based IoT approach. As a result, the producers and consumers of data are freely coupled in space, they do not have to know each other, in time, and they do not have to be available at the same time and in synchronization, asynchronous and non-blocking messages.

Typically, connected devices are severely restricted and connect to a gateway, which is directly connected to the Internet. However, most of the time this link uses relatively slow, last mile, last distance technology, such as digital subscriber line (DLS) or 3G / 4G, which makes it the bottleneck between devices. And the cloud, in terms of lag and performance. As the architecture scales, more resources become available, the number of services supported, and the power and spatial distribution of data producers and consumers increase toward the cloud. However, the latency from the end devices to the storage and service nodes also increases towards the top.

Advantages of Using Cloud Computing

Cloud computing offers the means to meet some of the requirements of IoT systems, these are [26, 33-35]:

Flexibility

Cloud instances are generally based on virtualized physical hardware in computer centers. Resources are pooled and can be used on demand, often with a pay-as-you-go model, where only actually used resources are billed. This aligns perfectly with the ever-changing requirements of IoT applications.

Reliability

Redundancy within and between computing centers can be used to create scalable and reliable services, such as distributed object storage. Basic distribution, storage and processing services can be conveniently provided using a cloud-based infrastructure.

Fast and Ubiquitous Access

Cloud computing centers are well-connected using private peers and multiple uplink transit providers. This allows ubiquitous and fast access to services from anywhere over the Internet.

Ease of Deployment

Cloud providers often offer readily available software components for custom solution development, which can be accessed through a well-defined API. Some vendors specifically target IoT use cases. This reduces both application time to market and development cost. There are also several specific use cases where cloud computing is not ready for IoT applications.

The limitations of cloud computing in the context of IoT can be summarized as follows:

High or Unpredictable Latency

They are fundamental requirements for many IoT tasks, such as in, devices commonly found in industrial automation, but also in other IoT use cases, such as home automation. As cloud data centers are primarily located where power is cheap, they are not located close to potential IoT users, adding unavoidable latency, as the physical distance between users and the cloud dictates the minimum latency, that can be achieved.

High Uplink Bandwidth Requirements

Gateways that do not have the bandwidth capacity to upload certain types of data from IoT devices to the cloud will not be able to use the cloud-based approach to storage and processing. For example, a value-added video analytics service may not be feasible as a remote cloud-based service, as the data to be transferred is too large for the available link. This is especially likely for rural areas or mobile connection, such as a 3G uplink.

No filtering or Aggregation within the Network

Some applications cover a large geographic space, while only an added value of the sensors is really important. For example, if the maximum temperature in multiple locations is identical, sending each sensor reading to the cloud will not be the most efficient solution. Instead, processing within the network could greatly reduce the amount of data that actually needs to be sent, processed, and stored in the cloud.

Uninterrupted Internet Connection is Required

Some applications, such as connected smart vehicles, can lose connection to the Internet and therefore also to the cloud. During network outages, the cloud approach would stop working and thus certain device functionalities would not run. Instead, local processing could be used to provide at least one alternate interim service until network connectivity is restored.

Since cloud providers are expected to respect user privacy and offer sufficiently secure services. However, there is no easy way to measure or monitor the security of cloud services, so those requirements cannot be easily verified and the provider must be trusted to some extent. Even if the provider is trusted, since the resources are virtualized, the containers of different device users are on the same physical machine, where software bugs could leak private data to third parties. And laws may require that certain data is not stored outside of certain legal areas, that it is not verifiable with most cloud providers.

These limitations imposed by the use of cloud computing motivate the need for additional technology that can mitigate these problems, especially in critical IoT applications. Computing in the fog appears to be a viable option in such an environment [30, 33, 36].

Although the benefits of cloud computing in the context of IoT are recognized by the industry and research communities, there are criticisms about storing and processing data in the cloud. In many use cases, the data consumer or service user is close to the data producer, but the data follows the path through the cloud. A related problem is the unnecessary load on Internet service providers (ISPs) and the additional delay introduced [36].

Unnecessary traffic could make communication on the network expensive or even prohibitive when there is no broadband connection available and alternative technologies must be used, for example mobile data links. This concerns both developing countries and rural areas where these types of devices must be deployed.

Fog computing is a term coined by the Cisco company, following a concept similar to cloud computing, which offers a highly virtualized pool of resources at the edge of the network. It provides computing, storage and communication services to nearby end users, as opposed to the cloud, which is generally located at the furthest point on the network. Therefore, the fog will have a widely distributed implementation, as well as a large heterogeneity of devices. The concept of fog can be illustrated as a cloud near the place or user of the particular use case.

Traditional content delivery networks (CDNs) share a similar concept of bringing data closer to the user, helping to meet the growing demand for streaming media traffic by placing data at the edge of the network (edge computing).

Microsoft has promoted a similar concept with its micro datacenter approach as an intermediate version to cloud and fog. The planned micro data centers are autonomous computing environments with computing and storage resources, which are connected to the Internet through high-speed connections. They basically follow the typical cloud approach, but scale the hardware closer to the edge of the network to avoid unnecessary delays. A customer can host dozens of servers in these micro-hubs that have terabytes of storage when combined. Instead of a central layer in the cloud, several hierarchical layers of nodes are introduced into the fog, which are increasingly closer to the edge of the network.

Gateways are now seen as part of an abstract fog layer. Since those devices are limited in terms of processing power, the cloud provides storage and processing capabilities when they are not sufficiently available in the fog. In general, instances in the fog may also be available on other network hardware, such as routers at ISPs, providing the means to analyze and process data within the network closer to the end user than in a centralized remote cloud. The most powerful fog nodes can also offer virtual machine provisioning.

Local processing on gateway devices is made possible by advanced IoT hardware, including from powerful smartphones or microcomputers. Most IoT devices still have power limitations, so it is common to use a gateway to connect to the Internet. Those gateways, on the other hand, are typically powered directly from the electrical grid and are powerful enough to take on some of the tasks that cloud services have traditionally offered, such as data processing and storage. There are different gateway devices that are currently used and that are used to interface with low-power sensors and offer local processing and storage.

The benefits of extending cloud computing to cloud computing closest to the IoT device.

Minimize Latency

Since cloud-computing centers are generally deployed where they cost less economically, the physical distance between the IoT device and the cloud service used can result in worrying latency. Analyzing data without transferring it and making decisions locally, or close to the data source, can greatly reduce the latency of all typical operations in the IoT ecosystem.

Improved Reliability

The IoT vision includes the use of sensor data for public safety or critical infrastructure. While most enterprise cloud service providers offer highly reliable computing centers with redundant network connections, storage, and processing infrastructure, the uplink to the cloud could easily be disrupted in such scenarios. It would be interesting to be able to do some of the processing locally as and option, or to exclusively use local processing.

Increased Privacy

Some IoT data will be confidential or required by law not to be stored outside of specific geographic boundaries of an administrative boundary. While cloud service providers are generally considered trustworthy, the user has no control over where the data is actually stored and who can access it. Nor can it be completely ruled out that, due to errors, third parties could illegally access confidential data. The local gateway or other nodes in the fog, on the other hand, can be reliable as they are under the control of the local operator. Of course, these could also be exposed to security vulnerabilities.

Conservation of Bandwidth

The uplink bandwidth of IoT gateways is often very limited, such as DSL or a 3G connection. It is not always feasible to transport large amounts of data from edge devices to the cloud. Performing data processing locally and only sending aggregates and previously filtered data to the cloud can significantly reduce uplink bandwidth. In this way, it is possible to deploy IoT systems that do not meet the exemplary conditions, since they are connected to the cloud through limited or intermittent connections. There are different possible use cases in which IoT applications can take advantage of fog computing, among which we have (47-49).

Smart Electric Network

It is a next-generation network, which aims to provide more effective load balancing and greater reliability, as well as lower electricity costs by automating the metering process. Smart meters collect and transmit information about electricity consumption, enabling more accurate pricing models based on actual supply and demand. Cloud computing can be used to store measurement information locally in such scenarios, where local gateways would act as the lowest level of storage. The fog nodes between the user end and the cloud would only be upgraded in batches, reducing the bandwidth requirement for smart meters.

Rather than relying on higher layers, such as the cloud layer, for advanced analytics, fog nodes close to the user could use such information to help customers change their behavior regarding energy use or to better predict energy use. Future demand and supply. Edge or fog computing could also be used to improve local power load balancing applications. Depending on the current price and local energy needs, the system can turn energy-intensive appliances on or off, or it could automatically switch them to different energy sources, such as solar or wind.

Vehicles Connected

They refer to techniques that provide wireless connectivity for vehicles that allow direct communication between the vehicles themselves and between the vehicles and the environment. The application that would benefit the most from fog-based approaches in that context, would be the automatic intelligent reaction to sensor readings found in cars. A smart traffic light could stop or slow oncoming traffic to avoid jams or accidents when multiple vehicles are detected braking. These use cases require communication between vehicles as well as local processing, as sending all sensor readings to a cloud is costly and introduces a delay that is not acceptable for timely reaction to traffic conditions. Local storage and data processing in the fog can help overcome those problems and enable those use cases.

Education

Students increasingly use devices such as computers, laptops or tablets for their studies. This allows you to study at your own pace and have the same information available at home as in the classroom. By monitoring student progress on these devices, teachers can collect real-time performance data on individual students and get actionable information on which students need more help. Analyzing performance data and storing additional course materials fundamentally pose the same challenges for the infrastructure as IoT data, which must also be stored and processed. Techniques in the fog can also improve the privacy of student data by not uploading sensitive data about their performance to cloud-based systems.

Health Care

The sensors can collect health information such as EKGs, temperature, or blood glucose level. Other physical monitoring sensors could detect if older people are following their daily routine; for example, they could monitor whether the person wakes up in the morning or eats regularly. Most of these applications have high reliability and strict latency requirements. In addition to that, privacy and regulations on patient data must be considered. Patient data could be transferred directly to physicians for diagnosis. Fog-based storage and processing could allow better monitoring of patients and seniors without sacrificing privacy and / or reliability.

Smart Buildings

In which the energy consumption of buildings can be optimized and the comfort of life and safety can be increased. These intelligent environments are possible thanks to the fusion of multiple technologies, such as temperature and humidity sensors among other sensors, ubiquitous connectivity and data analysis. Smart buildings could, for example, detect when no one is home and turn off the heating. Gas or air quality sensors could improve safety by giving a warning signal of poor air quality or unhealthy concentrations of certain gases, or even taking action on their own by opening windows to allow entry of air. Fresh air.

Of course, these actions can be activated through a cloud-based service; however, since the data producers and consumers are mostly local, the increased latency and traffic is unnecessary. A local fog-based system could use external data from cloud-based services, but analyze local sensor readings without sending them to distant clouds. As system reliability is critical in some use cases, it is important to note that fog-based services would continue to work in the event of intermittent internet connectivity.

Surveillance

In addition to intelligent video surveillance, it is based on cloud-based systems for complex video analysis. Instead of a human operator, a cloud-based service employs computer vision and pattern recognition algorithms to assess the scene. Other sensor readings can help with the recognition of potential threats. A fog-based system can help improve the detection and response time of such a system by avoiding the delay introduced when communicating with a distant cloud service. Multimedia data, in particular, is large and it is not always possible to send high-speed, high-resolution video to the cloud. Instead, the video can be analyzed locally, potentially at a higher resolution and speed than would be possible to send over the Internet uplink.

Wearables

The rise of wearable sensors, such as fitness monitoring sensors and smart watches, has led to a growing demand for processing sensor data, such as activity recognition based on accelerometer and gyroscope readings. The data have to be sampled at relatively high frequencies to derive meaningful activities. The activities themselves can be very private and must be protected against unauthorized access. The result of the recognition algorithm may be required with low latency in configurations where there is no internet connection available. In these configurations, local processing at nodes in the mist could be a solution, between avoiding computing on battery-powered devices and keeping data and processing close to the user.

Virtual Reality

In recent years, there have been several virtual reality solutions, such as the Oculus Rift, HTC Vive, and Google Cardboard. In the future, some of these devices may become wireless and portable. The amount of data that needs to be processed to make a compelling VR experience possible could potentially be dumped into the nodes in the mist, saving power and therefore battery power, while still having a small enough latency to unnoticed. Despite the advantages of fog, computing, different issues must be considered for the implementation of an IoT approach based on it, as well as integration with the current cloud-based model. Some of these challenges are (33-36).

Technological Interoperability

Since the seamless interaction between devices and systems from different vendors is a major challenge for IoT, as well as for fog-based extensions of IoT. There is still a strong lack of standards for communication protocols, both locally and for the uplink to the cloud. For example, to connect sensors to gateways, technologies used include Bluetooth Low Energy (BLE), 802.15.4 or ZigBee, or Wi-Fi (802.11). In addition, long-range wireless technologies are also being used, such as LoRaWAN or Sigfox.

Uplink protocols include proprietary technologies in addition to open pub / sub protocols such as Message Queue Telemetry Transport (MQTT), Extensible Messaging and Presence Protocol (XMPP), or Advanced Message Queuing Protocol (AMQP), and request / response protocols such as the Restricted Application Protocol (COAP). The protocols must be standardized and previously agreed for the IoT to be a reality. Also, techniques for storage and processing migration must be developed.

Semantic Interoperability

For interoperability, it is also necessary that the devices and software involved interpret the information collected, processed and shared in the same way and act according to the commands in a consistent way. A semantic model must be available for each aspect of the fog / cloud approach; This should not only be to understand the data, but also to express the requirements and limitations when processing or moving this data, including quality of service or privacy requirements. There is still a lack of knowledge about which ontologies may be suitable for these tasks. Semantic web technologies could also help improve device discovery or implement automatic reasoning.

Programmability

Data processing is of exceptional importance to the IoT ecosystem. Due to the variability of the requirements of event-based processing tasks, it is crucial to automatically relocate processing tasks between the cloud and fog nodes. However, it is not yet clear how the processing jobs should be defined. There is still a lack of knowledge about which programming language and which interfaces are required for IoT data processing, as well as to allow seamless downloading of tasks between different systems, potentially using different hardware architectures and different formats. In particular, a consensus has not yet been reached on whether to use an interface in the form of discrete functions or in the form of containers or virtual machine images.

Scalability

In the near future, the IoT will be made up of billions (or even trillions) of devices. The number of connected nodes will exceed the number of hosts on the Internet today by several orders of magnitude. Despite the problems that fog-based processing and storage can solve, it is still unclear how seamless interaction between devices behind different gateways should work. How large-scale devices should be discovered, where the log should be located in a system in the fog or in the cloud, or where the data should be located to minimize communication latency and increase performance, have yet to be found answered.

Resilience and Reliability

The fog-based approach is attractive for developers to deploy applications where permanent link to the cloud is not acceptable due to the potential for temporary outages. Some examples include industrial monitoring or emergency response systems.

From a business perspective, managing and obtaining information from the data generated by IoT devices is a challenge and a key to obtaining a competitive advantage against the competition. There are analytical solutions that extract structured and unstructured data, as they can help companies to obtain insights, not only from IoT device data, but also from the vast amounts of data publicly available on the web, social networks and computers, Blogs. These solutions, called big data, open a wide range of possibilities for organizations to understand the needs of their customers predict their demands and optimize resources.

Big data analysis is different and more powerful than the traditional analysis tools used by companies, it allows to find patterns and obtain intelligence from the data, translating them into a commercial advantage. However, big data works with what is often called a multi-V model, where each V stands for: Variety. Velocity. Volume. Veracity:

Where Variety. Represents the data types. Velocity. Represents the speed at which data is produced, processed and stored according to the analyzes to be performed. Volume. Represents the amount of data. And truthfulness. It represents how much the data can be trusted given the reliability of its sources.

Big data architectures are based on a flow processing perspective. Data flows are transferred to perform specific tasks or achieve the end goal. Typically, data is handled sequentially with tightly coupled predefined processing subunits, static data routing. This paradigm can be described as process-oriented or batch [59, 60].

A central coordination point manages the execution of subunits in a certain order and each subunit provides a specific processing output, which is used only within the scope of its own process, without the possibility of being shared between different processes.

This approach represents a major departure from traditional service-oriented architectures, where subunits are external web services invoked by a coordinator process rather than internal services. Big data applications generally interact with cloud computing architectures, which can manage resources and provide services to consumers. In the IoT realm, with millions of nodes capable of collecting data and generating information, the availability of efficient and scalable mechanisms for data ingestion, processing and persistence is crucial.

Big data techniques, which have been developed in recent years, address the need to process extremely large amounts of heterogeneous data for multiple purposes.

These techniques are primarily designed to handle large volumes, focusing on the amount of data itself, rather than providing real-time processing that is necessary in IoT.

Cloud computing has created the right scenario for big data analysis due to its scalability, robustness, and cost-effectiveness. The number of data sources, on the one hand, and the subsequent frequency of incoming data, on the other, have created a new need for cloud architectures to handle massive flows of information from IoT devices, thus producing a change in the big data paradigm to the big stream paradigm [59-61].

Various relevant IoT scenarios, such as industrial automation, transportation, sensor and actuator networks, require predictable latency in real time and could even change your requirements, for example in terms of data sources dynamically and abruptly. Systems oriented to large flows must react effectively to changes and provide intelligent behavior when allocating resources, thus implementing scalable cloud services. Dynamism and real-time requirements are another reason why big data approaches, due to their batch processing, are not suitable for many IoT scenarios.

The main differences between the big data and big stream paradigms are the nature of the data sources and the latency / real-time requirements of the consumers.

The Big Stream paradigm enables ad hoc, real-time processing to link incoming data streams to consumers. It offers a high degree of scalability, fine and dynamic configuration, as well as management of heterogeneous data formats. In summary, while big data and big stream systems handle massive amounts of data, the former focuses on data analysis, while the latter focuses on data flow management. The difference is in the meaning of the term big, which refers to the volume of data for Big Data and the rate of data generation for big stream.

This difference is also important in terms of the data that is considered relevant to consumer applications [60].

Conclusions

We live in a time where new medical devices are emerging, the industry in the health sector is growing thanks to technological advances; the diagnosis, treatment and monitoring of diseases and medical conditions are oriented towards the incorporation of development technologies created not only in clinical laboratories, but also in large corporations dedicated to the development and implementation of software.

Today, concepts such as nanotechnology, big data, wearables, are developed to monitor the health status of the general population and each person is used to having in their pocket, monitoring blood pressure, cholesterol levels, weight, index of body mass, up to the tracking of more advanced programmable biotech equipment that can keep the heart beating.

Wearables are those devices that we carry and that we get used to having, such as a wristwatch that shows the heartbeat and at the same time, reminds us of the day's agenda.

The interconnection seems to point to simple and ideal solutions to send reports and diagnoses in real time to the doctor. The objective is not only to carry out early clinical diagnoses, the goal goes further, it is to prevent serious health conditions, launching alerts in real time when something is not going well in our body.

The implications of devices and patients being linked to the cloud. The information is a key piece to determine trends, risk factors, daily habits that can improve or worsen a certain medical condition; the collection of data, big data, will help improve health schemes and programs, there will be real-time information on the areas of medical devices that require more attention and the results that previously took years to collect, measure, empty and publish, today they are obtained through fast and simple applications that we install on our mobile device.

Nanotechnology also has an important place in technological development, knowledge of matter at the atomic and nuclear level, allows the design of implantable devices that are ever smaller and less invasive, and we began to elucidate the results of the research, but the device industry Doctors are going through a stage with a panorama that perhaps now, we are not even able to imagine Therefore, the IoT is going to revolutionize the clinical laboratory of the future, as well as many other areas of companies and society.

References

1. Katrin Claire Leitmeyer, Laura Espinosa, Eeva Kaarina Broberg, Marc Jean Struelens (2018) The ECDC National Focal Points laboratory e-reporting survey group members. Europe's journal on infectious disease surveillance, epidemiology, prevention and control 26.
2. Cheng Jung Yang, Ming Huang Chen, Keng Pei Lin, Yu Jie Cheng, Fu-Chi Cheng (2020) Importing Automated Management System to Improve the Process Efficiency of Dental Laboratories. Sensors 20: 5791.
3. Ali K Yetisen, Juan Leonardo Martinez Hurtado, Barış Ünal, Ali Khademhosseini, Haider Butt (2018) Wearables in Medicine. Adv Mater 16: 30.
4. El Internet de las Cosas. En un mundo conectado de objetos inteligentes. Nº 15. Fundación de la Innovación. Bankinter. 2011.
5. El hospital del futuro (2019) El papel del hospital en una asistencia sanitaria centrada en el paciente. Un proyecto de la Sociedad Española de Medicina Interna para el Sistema Nacional de Salud. Elaborado con la colaboración de la Fundación IMAS. Sociedad Españo9la de Medicina Interna (SEMI) https://www.fesemi.org/quienes/semi/hospital-del-futuro
6. Tecnología IoT en el Sector Hospitalario. Informe Tecnológico. Quental www.quental.com.
7. Monográfico de transformación digital del Sector Salud. Revista de la Sociedad Española De Informática y Salud. 2016.
8. Ian Holland, Jamie A Davies (2020) Automation in the Life Science Research Laboratory. Front Bioeng Biotechnol 8: 571777.
9. Franklin R Borkat, Richard W Kataoka (1980) Laboratory Request Terminal for an Automated Clinical Laboratory. Proc Annu Symp Comput Appl Med Care 5: 529-533.
10. Callejas Cuervo M, González Cely AX, Bastos Filho T (2020) Control Systems and Electronic Instrumentation Applied to Autonomy in Wheelchair Mobility: The State of the Art. Sensors (Basel) 20: 6326.
11. Seungjin Kang, Hyunyoung Baek, Sunhee Jun, Soonhee Choi, Hee Hwang, et al. (2018) Laboratory Environment Monitoring: Implementation Experience and Field Study in a Tertiary General Hospital. Healthc Inform Res 24: 371-375.
12. Florentin Michel Jacques Bulot, Hugo Savill Russell, Mohsen Rezaei, Matthew Stanley Johnson, Steven James Johnston Ossont, et al. (2020) Laboratory Comparison of Low-Cost Particulate Matter Sensors to Measure Transient Events of Pollution. Sensors (Basel) 20: 2219.
13. Antonio Celesti, Armando Ruggeri, Maria Fazio, Antonino Galletta, Massimo Villari, et al. (2020) Blockchain-Based Healthcare Workflow for Tele-Medical Laboratory in Federated Hospital IoT Clouds. Sensors (Basel) 20: 2590.
14. Sapci AH, Sapci HA (2017) The Effectiveness of Hands-on Health Informatics Skills Exercises in the Multidisciplinary Smart Home Healthcare and Health Informatics Training Laboratories. Appl Clin Inform 8: 1184-1196.
15. Nižetić S, Petar Šolić, Diego López-de Ipiña González de Artaza, Luigi Patrono (2020) Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. J Clean Prod 20: 274.
16. Mateusz Daniol, Lukas Boehler, Ryszard Sroka, Anton Keller (2020) Modeling and Implementation of TEG-Based Energy Harvesting System for Steam Sterilization Surveillance Sensor Node. Sensors (Basel) 20: 6338.
17. Valentina Bianchi, Monica Mattarozzi, Marco Giannetto, Andrea Boni, Ilaria De Munari, et al. (2016) A Self-Calibrating IoT Portable Electrochemical Immunosensor for Serum Human Epididymis Protein 4 as a Tumor Biomarker for Ovarian Cancer. Sensors (Basel) 20: 2016.
18. Nidia GS Campos, Atslands R Rocha, Rubens Gondim, Ticiana L, Coelho da Silva, Danielo G Gomes (2020) Smart & Green: An Internet-of-Things Framework for Smart Irrigation. Sensors (Basel) 20: 190.
19. Isabela A Mattioli, Ayaz Hassan, Osvaldo N Oliveira, Frank N (2020) Crespilho. On the Challenges for the Diagnosis of SARS-CoV-2 Based on a Review of Current Methodologies. ACS Sens 5:3655-3677.
20. PA Laplante, M Kassab, NL Laplante, M Voas (2017) Building Caring Healthcare Systems in the Internet of Things. IEEE Systems Journal 2017: 72-75.
21. Islam SMR, D Kwak, MH Kabir, M Hossain, KS Kwak (2015) The Internet of Things for Health Care: A Comprehensive Survey. In IEEE Access 3: 678-708.
22. STF 505 TR 103 375 (2016) Smart M2M IoT Standards landscape and future.
23. Emmanuel Darmois, Omar Elloumi, Patrick Guillemin and

Philippe Moretto (2018) IoT Standards – State-of-the-Art Analysi. Analysing the IoT Standards Landscape 2018: 237-263.

24. Sivkumar Mishra, Biju Patnaik (2017) Development of an Internet of Things (IoT) Based Introductory Laboratory for Some of the authors of this publication are also working on these related projects: Multi objective stochastic network reconfiguration.
25. Jaimon T Kelly, Katrina L Campbell, Enying Gong, Paul Scuffham (2020) The Internet of Things: Impact and Implications for Health Care Delivery. J Med Internet Res 22: 20135.
26. Pastor Vargas Rafael, Llanos Tobarra, Robles Gómez A, Martin S, Hernández R, et al. (2020) A WoT Platform for Supporting Full-Cycle IoT Solutions from Edge to Cloud Infrastructures: A Practical Case. Sensors 20: 3770.
27. Poynder R (2016) Glossary of terms and expressions used in connection with The Internet of Things with a final section of related Standards. Haverhill: The Internet of Things Association (IoTA) 2016.
28. DaCosta F, Henderson B (2013) Rethinking the Internet of things: a scalable approach to connecting everything. Berkeley, CA: A press Open 2013: 1-94.
29. Abel Lozoya de Diego, María Teresa Villalba de Benito, María Arias Pou (2017) Taxonomía de información personal de salud para garantizar la privacidad de los individuos. El profesional de la información 26: 1699-2407.
30. Buyya R, Srirama SN (2019) Fog and Edge Computing: Principles and Paradigms. John Wiley & Sons 2019: 512.
31. Cirani S, Ferrari G, Picone M, Veltri L (2018) Internet of Things: Architectures, Protocols and Standards. John Wiley & Sons.
32. Perry L (2018) Internet of Things for Architects: Architecting IoT Solutions by Implementing Sensors, Communication Infrastructure, Edge Computing, Analytics, and Security. Packt 2018: 1- 780.
33. Bittencourt L, Immich R, Sakellariou R, Fonseca N, Madeira E, et al. (2018) The Internet of Things, Fog and Cloud Continuum: Integration and Challenges. Internet of Things 3: 134-155.
34. Bonomi F, Milito R, Zhu J, Addepalli S (2012) Fog Computing and its Role in the Internet of Things. En Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing 2012: 13-16.
35. Mohan N, Kangasharju J (2016) Edge-Fog Cloud: A Distributed Cloud for Internet of Things Computations. Cloudification of the Internet of Things (CIoT) IEEE 2016: 1-6.
36. Munir A, Kansakar P, Khan SU (2017) IFCIoT: Integrated Fog Cloud IoT: A Novel Architectural Paradigm for the Future Internet of Things. IEEE Consumer Electronics Magazine 6: 74-82.
37. Guth J, Breitenbücher U, Falkenthal M, Fremantle P, Kopp O, et al. (2018) A detailed analysis of IoT platform architectures: concepts, similarities, and differences. En Internet of Everything 2018: 81-101.
38. Guth J, Breitenbücher U, Falkenthal M, Leymann F, Reinfurt L (2016) Comparison of IoT platform architectures: A field study based on a reference architecture. Cloudification of the Internet of Things (CIoT) IEEE 2016: 1-6.
39. Razzaque MA, Milojevic Jevric M, Palade A, Clarke S (2015) Middleware for internet of things: a survey. IEEE Internet of Things Journal 3: 70-95.
40. Da Cruz MA, Rodrigues JJ, Sangaiah AK, A Muhtadi J, Korotaev V (2018) Performance evaluation of IoT middleware. Journal of Network and Computer Applications109: 53-65.
41. Paul Sanmartín Mendoza, Karen Ávila Hernández, César Vilora Núñez, Daladier Jabba Molinares (2016) Internet de las cosas y la salud centrada en el hogar. Salud Uninorte. Barranquilla (Col) 32: 337-339.
42. Kurniawan A (2018) Learning AWS IoT: Effectively manage connected devices on the AWS cloud using services such as AWS Greengrass, AWS button, predictive analytics and machine learning. Birmingham: Packt Publishing Ltd 2018.
43. Varga E, Mijić D, Drašković D (2018) Scalable Architecture for the Internet of Things: An Introduction to Data-Driven Computing Platforms. O'Reilly Media 2018.
44. Perry L (2020) IoT and Edge Computing for Architects: Implementing edge and IoT systems from sensors to clouds with communication systems, analytics, and security. Packt Publishing Ltd 2020.
45. Ravulavaru A (2020) Enterprise Internet of Things Handbook. Packt Publishing Ltd. 2018.
46. AWS IoT Analytics, Guía del usuario de AWS IoT Analytics, Amazon Web Services. https://docs.aws.amazon.com/es_es/iotanalytics/latest/userguide/analytics-ug.pdf
47. Culic I, Radovici A, Rusu C (2020) Commercial and Industrial Internet of Things Applications with the Raspberry Pi. Apress 2020.
48. Hassan QF (2018) Internet of Things A to Z: technologies and applications. John Wiley & Sons 2018: 1-704.
49. Lee I, Lee K (2015) The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons 58: 431-440.
50. Nath Shyam, R Stackowiak, C Romano (2017) Architecting the Industrial Internet. Packt Publishing Ltd 2017: 1- 360.
51. Anton Haro C, Dohler M (2014) Machine-to-machine (M2M) communications: architecture, performance and applications. Cambridge: Elsevier 2014.
52. Misic VB, Misic J (2014) Machine-to-machine communications: architectures, technology, standards, and applications. EE UU CRC Press 2014.
53. Cruz M, Oliete P, Morales C, González C, Cendón B (2015) Las tecnologías IoT dentro de la industria conectada 4.0. Escuela de Organización Industrial (EOI) 2015: 1-190.
54. González García, Antonio Jesús (2017) IoT: Dispositivos, tecnologías de transporte y aplicaciones. Cataluña: Universitat Oberta de Catalunya 2017.
55. Cirani S, Ferrari G, Picone M, Veltri L (2018) Internet of Things: architectures, protocols and standards. Nueva Jersey: John Wiley & Sons 2018.
56. Tsiatsis V, Karnouskos S, Holler J, Boyle D, Mulligan C (2018) Internet of Things: technologies and applications for a new age of intelligence. Academic Press 2018.
57. Guinard D, Trifa V, Mattern F, Wilde E (2011) From the Internet of Things to the Web of Things: Resource-oriented architecture and best practices. Architecting the Internet of Things Berlín: Springer 2011: 97-129.
58. Evdokimov S, Fabian B, Kunz S, Schoenemann N (2014) Comparison of discovery service architectures for the inter-

net of things. IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing IEEE 2010: 237-244.

59. Biron J, Follett J (2016) Foundational Elements of an IoT Solution. O'Reilly Media Incorporated 2016.
60. Kurniawan A (2018) Learning AWS IoT: Effectively manage connected devices on the AWS cloud using services such as AWS Greengrass, AWS button, predictive analytics and machine learning. Packt Publishing Ltd 2018.
61. Kashyap R (2019) Machine learning, data mining for IoT-based systems. En Handbook of Research on Big Data and the IoT. IGI Global 2019: 314-338.
62. Yaogang Wang, Li Sun, Jie Hou (2017) Hierarchical Medical System Based on Big Data and Mobile Internet: A New Strategic Choice in Health Care. JMIR Med Inform 5: 22.