The Connectivity and Security of the Sensors Combined with the Architecture Ensure a Reliable and Functional IoT.

Christos P. Beretas

Head professor of cyber security department of Innovative Knowledge Institute (Paris Graduate School), Paris, France
[1] c_beretas@yahoo.com
* Corresponding Author

ABSTRACT

In recent years, the rapid growth in electronics, computing and the growing needs of people for communication, automation, electronic transactions, and electronic conveniences has helped develop new technologies that have evolved in our lives to make it easier by simplifying communication with people around us and simplifying various online services. IoT is a trend that has begun with enthusiasm, is currently underway and will continue to evolve over the years. In developed countries in the world, especially in the USA and Europe, there are thousands of online devices that perform specific tasks daily, such as electrical water pumps, statistical data collection, network control, vehicle guidance, food supply, motion sensors, patient monitoring, etc There are so many IoT manufacturers that each manufacturer applies their own security way, or they do not even apply security, considering Android itself is capable of defining and automatically protect the IoT. The scientific community has put the emphasis on upgrading protocols and services, providing more capabilities but significantly ignoring the security of the infrastructure that will be installed an IoT.

KEYWORDS
Keyword_1;
Keyword_2;
Keyword_3;
Keyword_4;
Keyword_5

1. Introduction

IoT already counts 40 years of life, an idea that began several years ago as an idea that quickly gained the impression of many researchers, and over the years it has evolved so much that today is everywhere, from our homes to public institutions, from tools and vehicles to medicine and robotics [1]. In recent years, IoT has experienced significant growth, owing to the rapid development of computer science, physics, IT and electronics, which has resulted in a continued reduction in hardware / software costs, if we think that in most cases used open source software (Android), technologies that designed but not implemented with the advent of the IoT were implemented and merged so that new technologies were born and the services offered to people doubled [2]–[4]. This has resulted in increased data demand and management, so new communication protocols and service interfaces have been upgraded and created, which in a sense have reinforced users' confidence to choose to use an IoT [5]–[7].

The massive growth of such devices soon led to uncontrolled smart constructions that provide users with tempting services, however, with unquestionable security [8]–[10]. Previous studies have shown that a significant part of IoT offers low or no security at all. Most devices do not give the user access and control, so it's impossible to know the level of security offered by each device, each user buys such a device connects it to the internet and if is perform the desired functions they feel secure [11]–[14]. An IoT example is "Amazon Alexa" very well known in the USA, it does not provide system management access to the user, user's does not know the security features and level, can not set the security level, does not know if user's are vulnerable to attacks [15]–[18].

2. Method

They are getting more and more into our lives, everyday people are talking about them as more functions have been simplified with them [19]–[21]. It is a term that has been done around us every day. It is about IoT that exchanges daily hundreds of data not only with each other but with other networks of different levels and functions. They are wirelessly connected or wired with sensors or other devices, IoT devices that are able to provide us with help at home, in the office, in the industry, and wherever we

want [22]. All devices today have a processor or a microprocessor, such as electric ovens, credit cards, cars, etc. We inevitably drive a new digital revolution something that a few years ago looked like a dream [23]. There might not be the term IoT, but the term exists and clarifies how IoT differs from the Internet, IoT offers device-to-device communication, meaning that the human factor is not involved in communication. They are used for data transmission and distribution and not for data processing, so they do not have powerful processors and consume little electricity [24].

The purpose created IoT is the various sensors that can be connected to an IoT and transmit information such as the level of humidity of a home, then IoT depending on the type of connection and the purpose that is installed will promote appropriate to that message either to the internal network or to the Internet, that is to say Cloud. IoTs have a small storage space, memory, processor but are not computers. Their role is to collect data from the sensors around them and then forward these data to other networks or other IoTs [25]–[27]. As seen in Figure 1.1.1, devices support too many network architectures and exchange data through several communication protocols designed for them and designed to facilitate IoT communication with both different network technologies and different device architectures and operating systems, so an IoT to be able to communicate with a sensor around it with a data network or with another IoT can use one or more communication protocols.

Fig. 1. IoT Multiple Network Architecture and Protocols Support

As technology evolves, both the data collected by an IoT becomes user-friendly and directly accessible [28]–[31]. Smart phones have contributed to the success of IoT after developing software that allows the collection and analysis of data collected by an IoT on the Smart phone, so users can access sensors at different locations in a home at any time, by installing equipment on a space of interest to them can perform remotely, for example they can open and close the lights of a house from a distance, open and close a water pump from a distance depending on the heat ground humidity, to perform general work in a home based on the results of the sensors of a place that this data has been collected by the IoT [32], [33].

Such devices in our days are used everywhere, in hospitals, in buildings, in homes, in construction, in transport, etc.

In hospitals using special sensors, nurses and doctors can monitor patients and receive the data they care about in a center of management or even on their smart phones. Processes such as blood pressure,

glucose, and other tests are automatically performed by distance also real-time prevention and monitoring of patients in telemedicine is also remotely available, in both cases the patient feels safe that someone is actually being informed constantly for the his/her health status and the doctor has direct control and is informed in real time about the health status of the patient [34].

Sensors in building facilities can play two major roles, the first being event prevention and security. The second role is the proper energy management. Special sensors can be placed in a building to control the building's humidity and temperature, then these sensors will transfer through the IoT the data to a database usually in the Cloud where they will be transferred to a third system to evaluate or making a decision, the data can also be sent to a user's smart phone for information or decision. Also, in a building can be placed sensors of strange motion sensing, smoke detectors that depending on the level of smoke will act accordingly, water and gas sensors. Etc. All of the above are intended to prevent and respond immediately to emergencies.

There are dozens of sensors in homes, for example in the kitchen sensors can detect the temperature of the food and reduce the intensity of the oven, smart refrigerators that control their fullness and buy online products. Smart TVs that essentially turn a smart TV into a computer, light sensors that depending on the time or light in a room give the light to the house depending on the time or the light there is to change the volume, remote management by a smart phone the internal electrical devices.

The construction industry has benefited greatly from the use of IoT. The production process from the start of production to the end is closely monitored by sensors that at each stage of a process implementation and the transition process for a second phase is closely monitored to ensure smooth operation and high quality with as few as possible failures in material and quality . The production process of products and materials can adjust the production unit according to demand data, so we achieve a smooth production process without over-production of products that would not be sold afterward.

Finally, the transport industry is the one that everyday people come into constant contact with, intelligent cars with sensors that prevent possible accidents with people on the streets, light traffic signals that regulate traffic depending on the traffic of the vehicles. Smart cities that residents interact with IoT through sensors and machines such as ticket issuance and parking for their cars that use smart phones and sensors to inform drivers about parking spaces around them. Improve road congestion by informing motorists of traffic jammed roads and finding possible alternative ways. Tracking immobilized vehicles on a road network and informing the authorities on a case by case basis.

All of the above are included in the magical world of IoT. It's no coincidence that IoT and sensors are on the verge of delivering more and more capabilities to their users.

3. Results and Discussion

3.1. Functionality of Internet of Things

In standard information systems and processing systems, the process followed is storage of the data and then progressing in its processing, IoT is contrary to this philosophy, which is why it is different from the other technologies, IoT is a data gateway in real time transfers the data to other information systems by analyzing the data passing through the IoT, the data that it is processing is processing at that time, the data are continuous, unstopable and derived from the sensors connected to each IoT, in this way before the data collected by an IoT is stored in the Cloud or transferred to another network, they have already been processed and the results have been exported.

The infrmation generated by data processing significantly help prevent and respond to emergencies and decision-making in a timely manner, taking into account price analyzes, measurement results, where later by using special software applications automatically or consciously made by decision-makers.

An environment that has installed Internet of Things is as follows:

- Sensors installed according to the functionality they will offer.
- Actuators that, depending on the data collected and processed by IoT, will perform the corresponding functions.

- Wireless / wired data networks, these networks will take over the transfer of data / information from one IoT to another, linking IoT to other networks, and finally storing information in Cloud.
- Information systems that automatically make decisions according to information transferred from IoT to them.

Further analysis of the above entities:

Sensors associated with IoT someone can meet in urroundings whether it is home or is an organization or business, there are various kinds of sensors, such as stone-shaped sensors that are used in the army in areas where there is no human agent, there are sensors in the shape of stone which detect movements and the heat of man [35]–[38]. Other sensors are those that detect humidity, gas and liquid leakage, smoke, atmospheric sensors, etc. Sensor capabilities vary depending on the capability and the use of a sensor [39]–[42]. The data as sent by the sensors is automatically processed by IoT and then the results are displayed at a terminal whether it is a smartphone or a decision-making device based on the information it has. A typical example is the closure or opening of a hydroelectric barrier that performs this function automatically based on the information it has received from the IoT which analyzed the data collected by the sensors.

An IoT is unimpotant without the use of wired and wireless networks, including Sensor-Intelligent Devices - IoT communication protocols. Data processing performed by a IoT must then be transferred to the next stage of the decision making process, this stage need not lie within the IoT area, it may be located on the other end of the planet, for this reason, IoT offers support too many communication protocols that support the interconnection of many different types of networks for the smooth transfer of data independent of infrastructure [43].

Finally, companies and organizations often use IoT to perform functions and services where they host their information systems on the same place, for example an automated entry process to an information system following an event to be recorded by a sensor such as a biometric control palm detector [44]–[46].

Obviously, this data processing of sensors, data storage, and decision making pose some questions about the safety of IoT [47]–[49]. In order to increase user confidence in IoT, whether these users are home or companies or organizations, the security of the device itself must be as safe as possible to make the risk of violating and interfering with the data they process. It should be ensured how to secure the connection of sensors connected to the device, the devices that execute commands depending on the information, and finally how to connect to other Cloud networks and services. For a secure IoT network including classic links to information systems and web infrastructures, all necessary network and application security measures should be implemented at both IoT and network levels.

Nowadays, where data is transferred in multiple ways, the issue of privacy is put in place, when IoT around which too much data is needed, it is necessary to ensure interoperability, so new IoT security standards will have to be designed to meet the increased needs of users and the same will be tailored to the security needs of the new era. Implementation of ensuring interoperability and designing new safety standards should not affect the size of IoT. It should not be forgotten that the IoT does not have the computing power and capabilities of a computer, so it can not have the size of a computer, so increasing the size of an IoT in order to enhance its security by adding security mechanisms is out of the way and the purpose of IoT and should not be approached as this would be a huge failure.

An IoT device is practically non-existent if it is not properly connected to a sensor, the sensor is the one that feeds the IoT with data and makes it practically real. Sensors exist for almost everything, for example there are sensors for rain, moisture, ground, gaunt, gas, etc. Equally important are actuators which, depending on the information they receive from the IoT, will perform a process, These actuators to be connected to an IoT is not necessary, the user of IoT can determine to accept the information that is required for the personal analysis without the necessity of performing a process. All these connectivity of these devices that collect, process data, and expose features are called a smart device network, as these other devices work harmoniously and coordinated to achieve a goal. The question that one might think is how these other devices work together harmoniously and are not mistaken. In the world of IoT there is the uniqueness, each sensor and every intelligent device connected to the IoT does not depend

on the type of device, both the sensors and the intelligent devices are separated at unit level so that all these objects get some kind of addressing which should have the following characteristics.

- Addressing with a view to the future connection and expansion of the IoT network with another IoT network the connection to other information systems.
- A hierarchy should be maintained in the directions so that there is no future sophistication.
- The type of addressing should be such that it fits as much as possible with other information systems and networks to make connection with different technologies as easy as possible.

As illustrated below in Figure 2, each sensor connected to the IoT has unique addressing, informs the user of the disruptions and then communicates with other networks or systems.

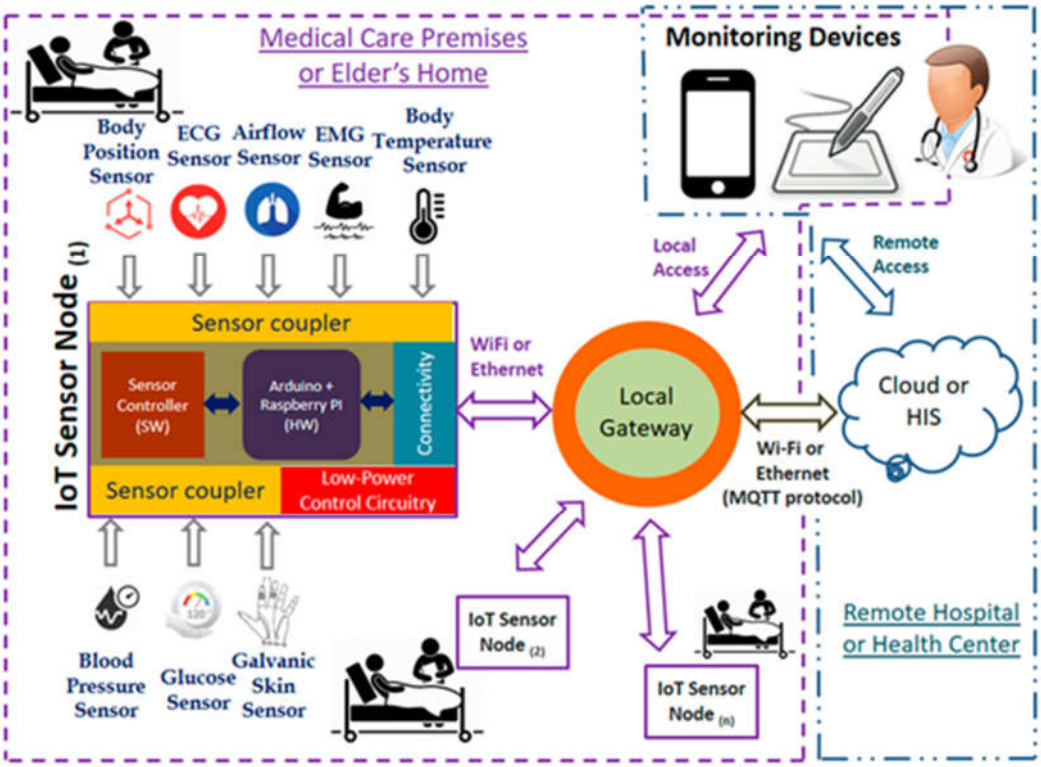

Fig. 2. IoT Sensors and Connection with Other Systems or Networks

Sensors are programmed to record an event for which they are installed. When the start of an activity starts and involves the use of the sensor, the sensor starts and records the event and transfers the data to the IoT. Then, after they are processed by IoT, they are transferred to Cloud to store, update users, and make decisions. Figure 3 below illustrates in stages the process of collecting data from the sensor, the processing stage, the stage of storage and decision making.

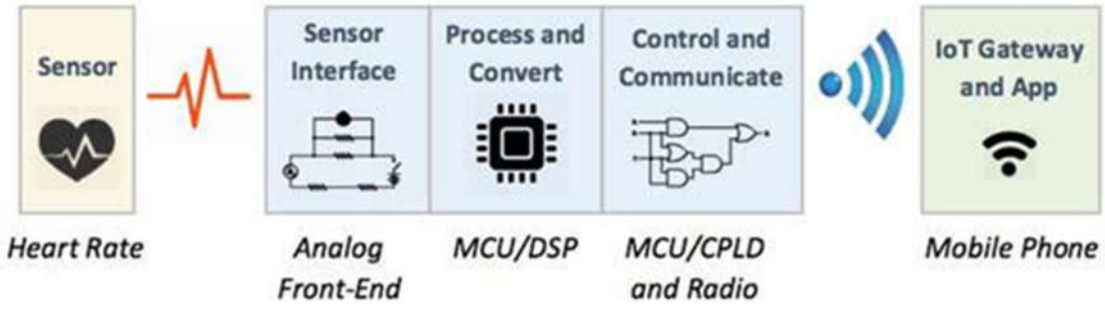

Fig. 3. IoT Stages from Sensors to Data Analysis and Decision Making

3.2. IoT in Business

How to use IoT between home and business is similar but also different, on the one hand, it is similar, because in both cases sensors are used, information is taken and decision maked, and on the other hand there are so many different things because in the field of businesses have security policies and a range of information systems and networks that all must harmonize with each other, a process that is more complicated than an IoT installed in a home. In the magical world of innovation and interoperability, there are not simple computing materials, but there are intelligent systems that are willing to serve us and simplify our work.

A device without hundreds of capabilities and a host of applications that would surmount it would be a failure, so in the world of IoT there are hundreds of applications that connect other devices and sensors, as the world embraces this new technology and the software that the framework evolves while offering additional capabilities, this has the effect of changing the way of manage, control, and develop of products and services as it changes their operating mode and increases operating efficiency. Figure 4 illustrates how an IoT with the appropriate software can improve the efficiency of a business.

Fig. 4. IoT in Business

The analysis of the above diagram shows the significant benefits of the use of IoT that enables the transformation of information systems and networks through automation [50]–[53].

Monitoring the process of producing products using appropriate sensors helps in organized and high-level production as there is interaction between actuators. This new model of production enables us to predict customer requirements and whether they are satisfied so we can have product invoices depending on the customers' demand.

In the modern professional world, IoT can not only contribute to productive development and monitoring, but can also help to solve important decisions such as viability studies, long-term business studies, project management, financial analyzes, etc. Automated tools and machines pass orders from IoT to perform work while reducing labor costs and increasing production while creating an environment for organizing the entire production process In every step of creation and processing

special sensors continuously monitor the implementation process and if something in the whole process does not go well immediately activate the automatic correction process, reducing the danger for appreciable products.

Finally, an IoT is really so smart that of course another sector has contributed to it, this is the field of artificial intelligence. IoT can build a lot of things, literally turn into an information and decision-making information center. Such devices are the ones that someone can discuss with them, ask them for things that interest, then they will look for answers from either a Server or the Internet or they will communicate with a sensor to receive data and provide information back, and of course the voice command to perform any work, such as Amazon Alexa, non-reverting aircraft, and the smart car that drives without a driver.

3.3. IoT in Smart Homes and the Risks

Undoubtedly is a technological revolution that has certainly focused on the interest of software development companies, companies of IT, hardware design, networks and artificial intelligence [54], [55]. A technological revolution that started a few years ago and has evolved rapidly, thanks to the technological evolution of IT and networks [56]. It is a combination of many communication protocols, sensors and other intelligent technologies, the correlation between smart technologies, networks and services that all together complete processes in order to achieve the result for which they were installed. In advanced technology countries, both simple users and industry use IoT where sensors are simplified and automated at home and in industry, there is continuous monitoring, control and prediction of product failure for the benefit of efficient production of high quality products and control production at each stage of product processing / production. Someone could well think and say that all this is fantastic and that we have solved the problem of organization, easy life without further thoughts and worries since everything is done automatically. An IoT in an intelligent house could literally regulate everything, using sensors and appropriate software could talk with a human person, as well as someone could appropriately entice all that security and literally take full control of the premises of a home with consequences from minimal to catastrophic including the complete destruction of a home [57], [58].

Several security advisors expressed their concerns about the safety of IoT a few years ago was something new and unknown in our days is something very familiar, complex, with many possibilities, connected to any type of network virtually unlimited, as an architecture can be gigantic and spread in quite large areas, receiving information from hundreds of different sensors where practically it can handle everything [59]–[62]. In a home, an IoT with the right sensors can control everything, such as filling a pool, automatically watering the garden according to the temperature and humidity of the ground, lighting the house indoors and outdoors by taking data from the sensors according to the actual illumination that exists, the disbelief and closing of the doors by taking data from the sensors and the identification of the human voice. The management of electrical appliances in the kitchen, temperature control in the oven and cooking based on the food found, water management using sensors that detect the real need for water and prevent over-consumption, control of hot water and electric power support if the water is not hot enough to reach the desired temperature levels. The above are just a few examples of using IoT, as easily as they sound, they are also dangerous, as long as we think about two things, the first is that IoT have access to the internet, every device connected to the internet is vulnerable to attacks. Secondly, if at some point in the IoT infrastructure it is violated, then the attacker could access all of these devices in a home and manage them as attacker wants. Based on the above, if there are no techniques and methods of confidentiality and validity at operating system level, none IoT is safe enough for the simplest reason that IoT play in different roles, connect to complex networks, include sensors from different manufacturers and different capabilities, mass gathering and processing of data, and then sending these data over networks to other platforms and services [63].

When talking about the protection and safety of an IoT, we should always be intimidating its self-protection and the guarantee of its operating system without interference from third parties. Let's analyze the risks further [64]–[66].

As described above, IoTs can significantly improve the quality of life of humans [67], [68]. The security of an IoT is a matter of little concern with the services it offers, most users believe that connecting such a device to their network is safe while others are wondering why someone should try to break their own IoT since they have nothing important to hide from the others and the attackers do not

have to win something to boast that they have committed a major violation of an IoT [69], [70]. Of course, all this is a mistaken thought and logic because we can not know the intentions of every man and even the neighbor thought. Let's analyze the level structure of an IoT. Each IoT is divided into 3 internal levels:

- Interaction with its sensors.
- Interaction with the Internet or other local networks and devices.
- The level of data publishing, whether it is a cloud application. A device that performs functions in conjunction with the data processed by the IoT.

Further analysis of the above levels of an IoT indicates separately for each level the risks and dangers that exist. Below, the risks and dangers are thoroughly analyzed.

- There must be a secure connections between the sensor and the IoT to prevent fake sensor combinations, this involves applying an appropriate security policy to ensure that the specific sensor is the one to be and that through it the sensor will interact with the IoT data in a secure manner. It should be borne in mind that the guarantee of the data that will interact with IoT with the sensor should be ensured because, on the basis of these data, decisions will be made.
- Storing the data is very important, and their perception could feed users with false data. The IoT should use secure and encrypted data transfer methods, storage space must also be safe, any tampering of the storage site poses a risk to both the data and the IoT itself. Creating a secure parallele storage system could control and restore fake files and let users know about it.
- When transferring the data, some kind of attack on the IoT network, whether can be a man in the middle attack or can also come from the internet. Therefore, an algorithm for self-protection of the IoT network is needed. There are some algorithms that are used for data accurancy, but without the right security policies they can not do much.
- The kernel of an IoT is a red flag for attackers, it could hide a malware and loging forever the habits, data, and peculiarities of each user, giving the possibility to external attackers to create an online user profile and be able to know everything from its transitions, lifestyle, and especially personal data.
- An incorrect security policy, a wrong software, a vulnerable sensor could "burn a home". Literally, they could burn a house, if a sensor had been tampered by an outside attacker, it could affect, for example, a sensor who is responsible for oven temperature, an attack would probably have caused the overheating of the oven to provoke fire. And if assuming that there was a fire alarm sensor connected to IoT in the house, then an attacker might well be able to deactivate it.
- Unauthorized users should not have access to IoT data management, operation, and publishing, the metadata often revealing important data sources. Authorized users should be granted partial access per level and not full access everywhere. Providing full access management everywhere at all levels then a DDOS attack could give complete access.
- Most of the security techniques that have been created are mainly aimed at the accuracy of the information transferred to the IoT network. Thinking that in case of set-up elements are the sensors and the storage media, the possibility of affection of the operating system remains second degree, a malware could work for years and log user habits, it will be a back door for the attackers, a back door of violation of human privacy.
- The use of default features by the manufacturer itself makes it a vulnerable IoT network structure, anyone who has physical access and knows the IoT model is easy to try to access by identify for its factory settings and factory passwords. This is a very serious attack, the first thing people have to do is change the default password and in some cases the default settings.

- User accounts with incorrectly restricted permissions, no password, access to services without user authentication, are red shield for IoT security, can easily break the security of the IoT network that depending on the type of installation in a home will also have consequences.
- When an IoT device is installed in a home in which there is a computer network that interacts with the IoT, should be ensured the harmonic communication with each other. If the computing network is unsafe then easily can break an IoT security. An IoT can not protect a vulnerable computing network, and a vulnerable computing network can not protect an IoT.
- It is important that where they store the data either if they will be stored locally on the premises, so there should be a way of data accurancy and backup, while in the case of Cloud the physical access is not permitted, should be ensured encryption of data information there, while is importan to creating a recovery plan for information where something goes wrong.
- The management of an IoT through a web environment is the backdoor of an IoT network mainly through Wi-Fi networks. The violation of a Wi-Fi and then access to the home network of the home allows external attackers to try illegally entering the IoT device through its web console, where any successful access, the attackers would have full control over the functions through the sensors throughout the home.

The above risks and dangers are the ones that someone should take care of and think about when installing an IoT in a home [71]. The security of a network such about an IoT security is not easy, especially when it comes to other types of networks and other IoT devices. The current security situation of an IoT has grown quite a bit, but not to a great extent to the safety of an IoT, most techniques focus on data security and encryption and not on IoT"s own protection. Its growth is rapid and will remain an upward course for years to come. Users have loved it, and every day new companies are part of the list that wants to upgrade their equipment for more productive product creation process, also the demand for creating smart homes is growing, the power of the artificial intelligence has been enter in our life, user-friendliness and automation is especially eager for new users.

3.4. Sensors Technology

The sensors used by IoT are categorized into unstructured distributed systems but differ from other unstructured distributed systems due to their specificity being subject to energy, computational power, and diversity constraints in communication protocols [72]. In Figure 5 observing the structure of the sensors as they interact with each other [73].

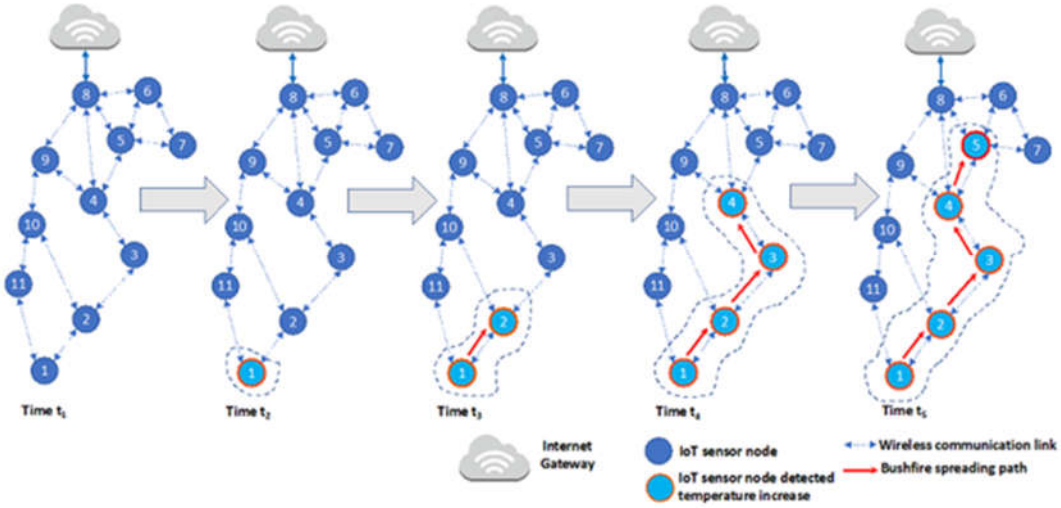

Fig. 5. IoT Sensors Network

There are two types of sensors, immovable - stationary sensors that are positioned at a stable point, do not move and record data always from the same point, but there are also mobile sensors that record continuous data as well as immovable - stationary data [74]–[76]. However, sensors with a specificity, mobile sensors are equipped with positioning systems, the purpose of the sensor communication with IoT is not only valid data but it plays a very important role the data transmission speed. Sensors are electronic devices that act as an interface between the physical and electronic worlds [77]–[79]. The sensors monitor the events taking place in the natural world and convert this data into an electrical signal, whereby the IoT is properly processed by the electrical signal according to the settings and options set by actuators managed by the IoT undertake to execute the commands they receive as shown in Figure 6 below.

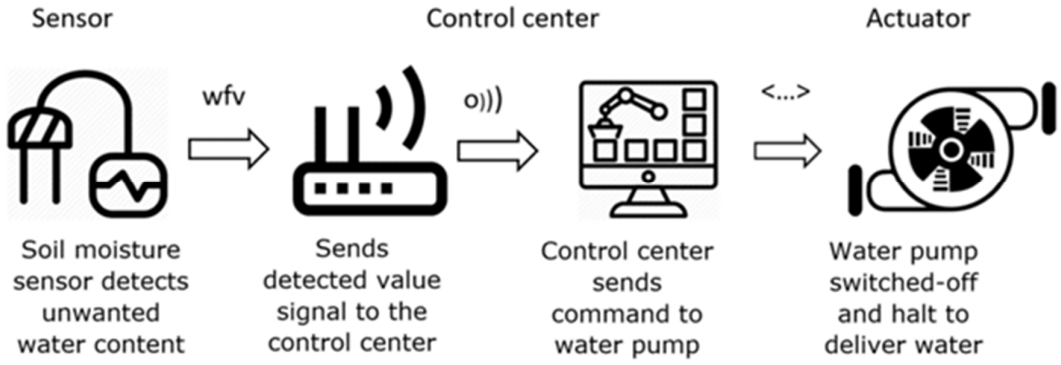

Fig. 6. Sensor to Actuator Flow

The basic function of a sensor as mentioned above is to monitor a physical phenomenon and record it in an electrical signal but this electrical signal must be compatible with other electronic devices in order to be read and recognized. The sensor output signal format does not contain any standard data output and the output data may be in various forms, such as current, voltage, or some density characteristics. The sensors can and do convert energy into electricity, but they do not convert generic energy into other energy, instead actuators receive electricity at the input to execute an action or activate a mechanism. The characteristics of the sensors are described below and highlight the high specifications and requirements.

- The event detection time, the event detection time relative to the recording time in combination with the output time.
- The ability of the sensors to return to their original recording state after the response time and output of the output signal is converted, and vice versa it takes some time for the input signal response system to return. That is, it takes some time for the input and output signal to return to its original value.
- The measurement of the speed of the physical input signal with the electrical output signal mainly in the form of a pulse graph is used to evaluate a sensor.
- The sensitivity of a sensor to timely perceive a physical event and the speed to convert it into a digital signal. How sensitive a sensor is is determined by the sensitivity of recording a physical input signal with the output of the output signal.
- The ability to record multiple input signals at the same time and convert them to digital signal without errors and misunderstandings. Simultaneous recording of many physical events beyond the capacities of the sensor mainly causes errors and malfunctions.
- Noise generated by the sensor or external factors affect the sensor. The noise coming from the sensor affects the output signal, the general noise generally affects the sensor, that is, both the physical input signal and the digital output signal. Noise is a common problem as almost all electronic devices produce some kind of noise.

- Depending on their cost and capabilities, the sensors may also include a micro controller that processes the physical input data and outputs digital output ready information, thereby reducing the time required to process the digital output signal and convert it into information.

The following diagrams 7 and 8 show the sensors without a microcontroller and with a microcontroller.

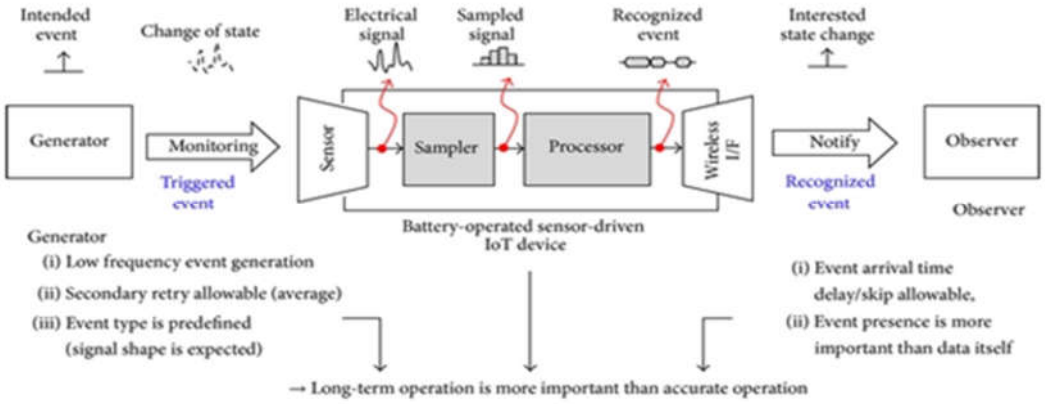

Fig. 7. Standard Sensor

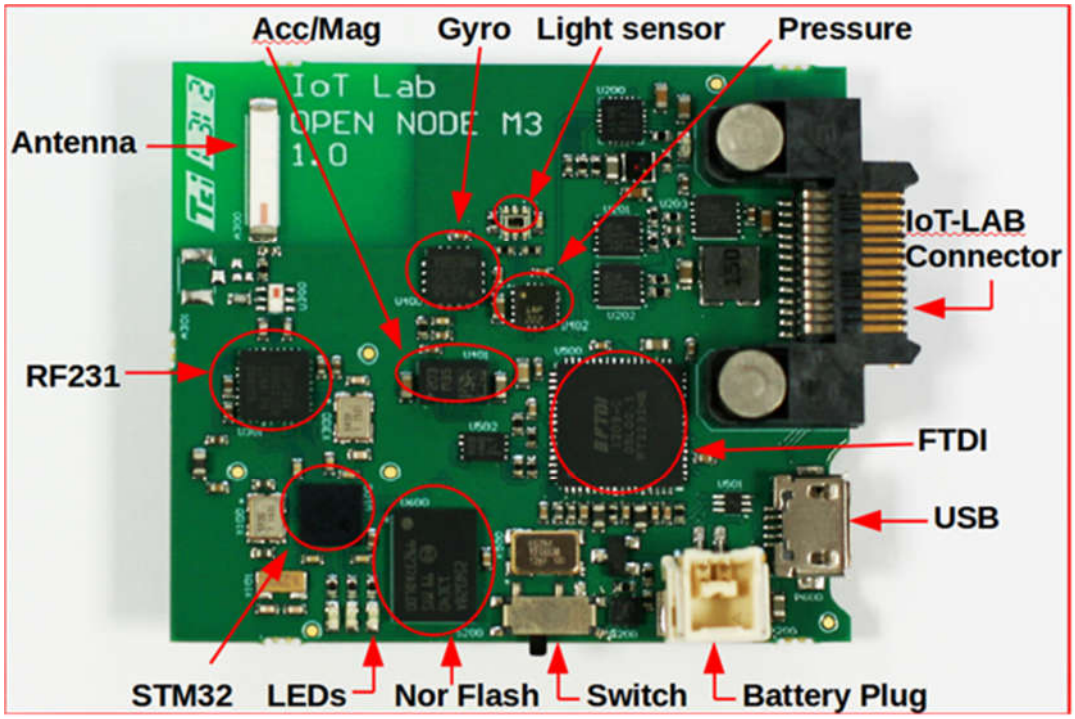

Fig. 8. Sensor with Micro-Controller

Sensors incorporating a microcontroller are more reliable than simple sensors, and they also outperform the integrity of the information and the very high reliability they offer. A microcontroller sensor is capable of repairing errors and metrics, controlling its own operation when it is not possible to physically record an event it does not record it in order to avoid the possibility of a misleading result, this is very important because the sensors they provide the user with ready information, does the information need to be reliable, in addition the ready information provided by the sensor to the user does the information and the whole system smarter and more operating and reliable because the

connection to other systems and networks are more convenient. One particular feature of microcontroller sensors is the ease of interconnection with other networks that are complex and otherwise there would be a problem using a classic sensor. Micro-controller sensors are able to connect to complex networks thanks to the ability to self-identify on the network, so different types of devices can exist in a network that can work together seamlessly. Particularly, microcontroller sensors cost more than traditional sensors, so there is also the limitation of climate change and the environment, in general, microcontroller sensors cannot be fitted everywhere, generally they need a protected environment from humid and water, so they need some more attention to their area and how to install them. Finally, because they contain a micro controller, and a multitude of electronic circuits, they require more electricity to operate. to work. In an environment where energy consumption and space analysis should all be taken into account for the proper functioning of the sensors and their performance.

3.5. Sensors Installation

When referring to a network of sensors, we are referring to a network consisting of smart devices that could be named "nodes" that exchange data between them. Each sensor in the area where it is installed observes and records a particular event, the data gathering from the other sensors will help to present a complete picture of the kind of interest the user has, which will then be captured based on this image. Decisions. The following characteristics must be taken into account when purchasing and installing the sensors.

- The cost of purchase.
- The geographical environment and weather conditions.
- Energy consumption and supply.
- The speed of data processing.
- The ability to store data is the ability to cache.
- Supported internet connection speed.
- Supported protocols.
- Expandable capabilities with other networks and different network topologies.

The sensors communicate wirelessly or wired and wireless, that is, hybrid independent of physical means of communication, that is, regardless of transmission via fiber optic or copper cable. Usually the sensors that are in an area that is home or in the business are the wireless, collecting the data automatically and then forwarding it automatically and wirelessly to local systems either to actuators or to cloud systems over the internet. When there are enough sensors in an area to extract an individual result, everyone needs special distributed processing protocols with the most significant advantage of noise reduction due to the reduction of the sensor distance from the signal source, the nodes are closer and closer to each other thus the required communication power is lower as shown in Figure 9 below.

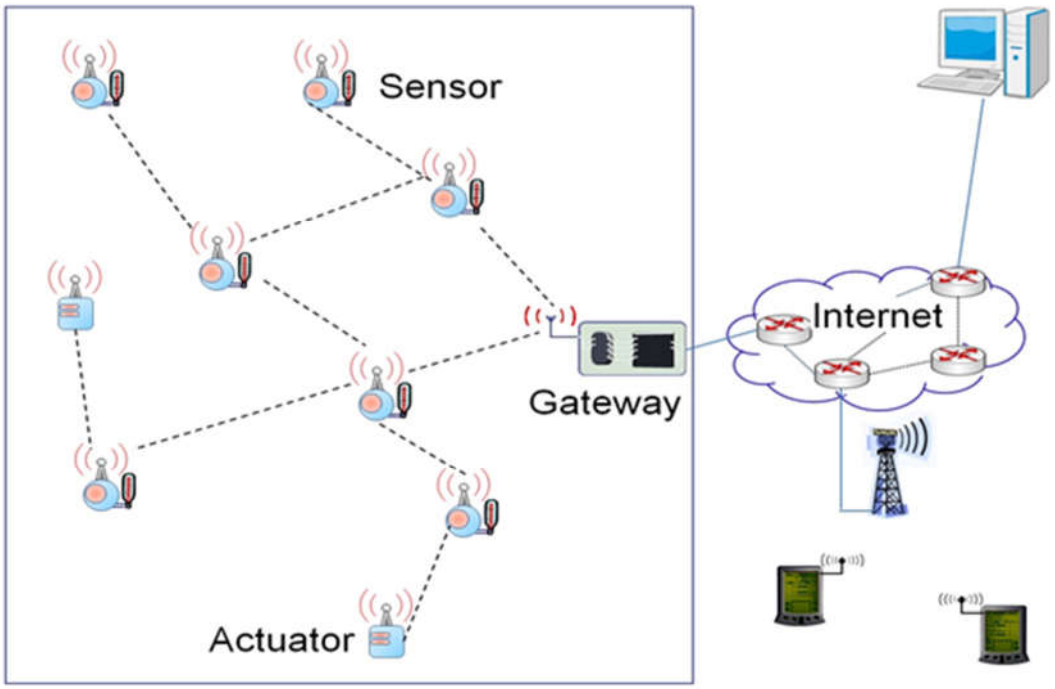

Fig. 9. Network with Sensors – Actuators

Distributed sensor networks are easy to deploy, have significantly fewer failures, node communication is easier, and communication protocols are efficient in terms of performance, physical detection is easier and more reliable, and ultimately energy saving [80]–[83]. A network of sensors can connect to other systems and networks within the same area using known communication protocols, or through a gateway it can connect to other external networks through known communication protocols also used on the Internet [84], [85]. The microcontroller sensor interface enables both other Internet services connecting to the IoT and the end user to have readable information ready to be managed, so this information lends itself well to computer networks and decision centers since it is a good if artificial intelligence is applied for decision making, as shown in figure 10 the information is extracted from the sensors then analyzed and then passed through artificial intelligence automatically the decisions to execute actions.

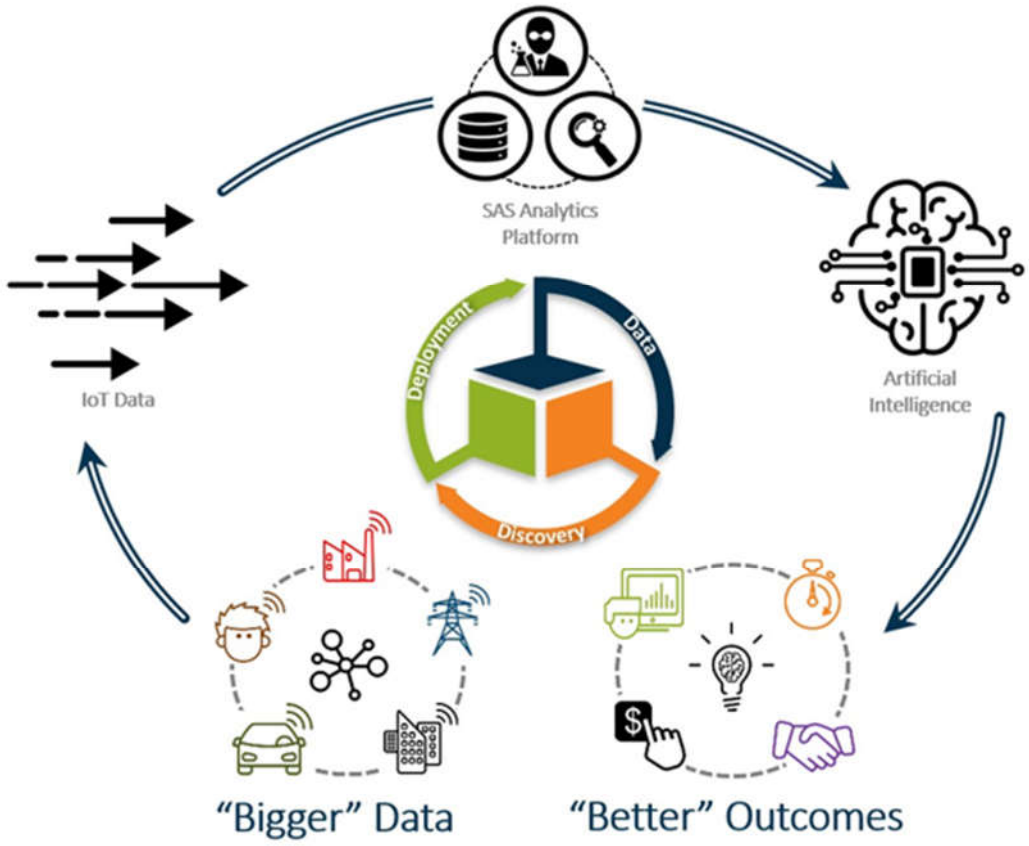

Fig. 10. IoT Decisions by Using Artificial Intelligence

Sensor software as well as any software used from physical data recording to final data analysis should be dedicated to this task and make full use of the resources available and managed properly to achieve energy savings. The speed of collecting, storing and processing data from the sensors directly affects the way analyzing and make decisions.

4. Conclusion

The purpose created IoT is the various sensors that can be connected to an IoT and transmit information such as the level of humidity of a home, then IoT depending on the type of connection and the purpose that is installed will promote appropriate to that message either to the internal network or to the Internet, that is to say Cloud. IoTs have a small storage space, memory, processor but are not computers. Their role is to collect data from the sensors around them and then forward these data to other networks or other IoT devices support too many network architectures and exchange data through several communication protocols designed for them and designed to facilitate IoT communication with both different network technologies and different device architectures and operating systems, so an IoT to be able to communicate with a sensor around it with a data network or with another IoT can use one or more communication protocols.

Acknowledgment

Special thanks to the internal funder for community service from the cyber security department of Innovative Knowledge Institute, Paris.

Author Contribution

The activity plan in order to the connectivity and security of the sensors combined with the architecture ensure a reliable and functional IoT.

Funding

Special thanks to the internal funder for community service from the cyber security department of Innovative Knowledge Institute, Paris.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] K. Lova Raju and V. Vijayaraghavan, "IoT Technologies in Agricultural Environment: A Survey," Wirel. Pers. Commun., vol. 113, no. 4, pp. 2415–2446, Aug. 2020.

[2] E. Navarro, N. Costa, and A. Pereira, "A Systematic Review of IoT Solutions for Smart Farming," Sensors, vol. 20, no. 15, p. 4231, Jul. 2020.

[3] A. Vangala, A. K. Das, V. Chamola, V. Korotaev, and J. J. P. C. Rodrigues, "Security in IoT-enabled smart agriculture: architecture, security solutions and challenges," Cluster Comput., vol. 26, no. 2, pp. 879–902, Apr. 2023.

[4] I. M. Benseñor et al., "Urinary iodine and sodium concentration and thyroid status in the Brazilian Longitudinal Study of Adult Health (ELSA-Brasil)," J. Trace Elem. Med. Biol., vol. 68, p. 126805, Dec. 2021.

[5] C. Maraveas and T. Bartzanas, "Application of Internet of Things (IoT) for Optimized Greenhouse Environments," AgriEngineering, vol. 3, no. 4, pp. 954–970, Nov. 2021.

[6] E. Özbilge, Y. Kırsal, and E. Çaglar, "Modelling and Analysis of IoT Technology Using Neural Networks In Agriculture Environment," Int. J. Comput. Commun. Control, vol. 15, no. 3, Apr. 2020.

[7] H. Mori, J. Kundaliya, K. Naik, and M. Shah, "IoT technologies in smart environment: security issues and future enhancements," Environ. Sci. Pollut. Res., vol. 29, no. 32, pp. 47969–47987, Jul. 2022.

[8] M. Kassim, M. Z. Zulkifli, N. Ya'acob, and S. Shahbudin, "IoT System on Dynamic Fish Feeder Based on Fish Existence for Agriculture Aquaponic Breeders," Baghdad Sci. J., vol. 18, no. 4(Suppl.), p. 1448, Dec. 2021.

[9] S. Vyas, M. Shabaz, P. Pandit, L. R. Parvathy, and I. Ofori, "Integration of Artificial Intelligence and Blockchain Technology in Healthcare and Agriculture," J. Food Qual., vol. 2022, pp. 1–11, May 2022.

[10] Y. Xun and G. Ren, "Smart Garden Planning and Design Based on the Agricultural Internet of Things," Comput. Intell. Neurosci., vol. 2022, pp. 1–11, Jan. 2022.

[11] G. S. Pandi (Jain), S. Shah, and K. H. Wandra, "Exploration of Vulnerabilities, Threats and Forensic Issues and its impact on the Distributed Environment of Cloud and its mitigation," Procedia Comput. Sci., vol. 167, no. 2019, pp. 163–173, 2020.

[12] A. Konkin and S. Zapechnikov, "Privacy methods and zero-knowledge poof for corporate blockchain," Procedia Comput. Sci., vol. 190, pp. 471–478, 2021.

[13] C. Verdouw, H. Sundmaeker, B. Tekinerdogan, D. Conzon, and T. Montanaro, "Architecture framework of IoT-based food and farm systems: A multiple case study," Comput. Electron. Agric., vol. 165, no. July, p. 104939, Oct. 2019.

[14]P.-E. Dossou, "Impact of Sustainability on the supply chain 4.0 performance," Procedia Manuf., vol. 17, pp. 452–459, 2018.

[15]J. C. Pinheiro, P.-E. Dossou, and J. C. Junior, "Methods and concepts for elaborating a decision aided tool for optimizing healthcare medicines dispatching flows," Procedia Manuf., vol. 38, no. Faim 2019, pp. 209–216, 2019.

[16]K. Haricha, A. Khiat, Y. Issaoui, A. Bahnasse, and H. Ouajji, "Towards smart manufucturing: Implementation and benefits," Procedia Comput. Sci., vol. 177, pp. 639–644, 2020.

[17]T. T. Aung, A. M. Thaw, N. A. Zhukova, T. Man, and V. . Chernokulsky, "Data processing model for mobile IoT systems," Procedia Comput. Sci., vol. 186, pp. 235–241, 2021.

[18]N. Surantha and W. R. Wicaksono, "Design of Smart Home Security System using Object Recognition and PIR Sensor," Procedia Comput. Sci., vol. 135, pp. 465–472, 2018.

[19]M. Haras, M. Markiewicz, S. Monfray, and T. Skotnicki, "Pulse mode of operation – A new booster of TEG, improving power up to X2.7 – to better fit IoT requirements," Nano Energy, vol. 68, p. 104204, Feb. 2020.

[20]N. N. Srinidhi, S. M. Dilip Kumar, and K. R. Venugopal, "Network optimizations in the Internet of Things: A review," Eng. Sci. Technol. an Int. J., vol. 22, no. 1, pp. 1–21, Feb. 2019.

[21]A. Galal and X. Hesselbach, "Nano-networks communication architecture: Modeling and functions," Nano Commun. Netw., vol. 17, pp. 45–62, Sep. 2018.

[22]L. R. Saragih, M. Dachyar, and T. Y. M. Zagloel, "Implementation of telecommunications cross-industry collaboration through agile project management," Heliyon, vol. 7, no. 5, p. e07013, May 2021.

[23]H. Maddar, W. Kammoun, and H. Youssef, "Effective distributed trust management model for Internet of Things," Procedia Comput. Sci., vol. 126, pp. 321–334, 2018.

[24]N. M. Kumar, "Blockchain: Enabling wide range of services in distributed energy system," Beni-Suef Univ. J. Basic Appl. Sci., vol. 7, no. 4, pp. 701–704, Dec. 2018.

[25]O. Debauche, S. A. Mahmoudi, S. Mahmoudi, and P. Manneback, "Cloud Platform using Big Data and HPC Technologies for Distributed and Parallels Treatments," Procedia Comput. Sci., vol. 141, pp. 112–118, 2018.

[26]J. I. Hur, L. C. Smith, and B. Dunn, "High Areal Energy Density 3D Lithium-Ion Microbatteries," Joule, vol. 2, no. 6, pp. 1187–1201, Jun. 2018.

[27]M. Wetzels, I. Ayoola, S. Bogers, P. Peters, W. Chen, and L. Feijs, "Consume: A privacy-preserving authorisation and authentication service for connecting with health and wellbeing APIs," Pervasive Mob. Comput., vol. 43, pp. 20–26, Jan. 2018.

[28]I. Shabani, T. Biba, and B. Çiço, "Design of a Cattle-Health-Monitoring System Using Microservices and IoT Devices," Computers, vol. 11, no. 5, p. 79, May 2022.

[29]Á. B. da Rocha, E. de M. Fernandes, C. A. C. dos Santos, J. M. T. Diniz, and W. F. A. Junior, "Development of a Real-Time Surface Solar Radiation Measurement System Based on the Internet of Things (IoT)," Sensors, vol. 21, no. 11, p. 3836, Jun. 2021.

[30]M. S. Farooq, S. Riaz, A. Abid, T. Umer, and Y. Bin Zikria, "Role of IoT Technology in Agriculture: A Systematic Literature Review," Electronics, vol. 9, no. 2, p. 319, Feb. 2020.

[31]C. Coccaro et al., "Consumption of iodized salt may not represent a reliable indicator of iodine adequacy: Evidence from a cross-sectional study on schoolchildren living in an urban area of central Italy," Nutrition, vol. 32, no. 6, pp. 662–666, Jun. 2016.

[32]J. Ngounda, J. Baumgartner, M. Nel, and C. M. Walsh, "Iodine status of pregnant women residing in the urban Free State Province of South Africa is borderline adequate: The NuEMI study," Nutr. Res., vol. 98, pp. 18–26, Feb. 2022.

[33]K.-T. Tang et al., "Iodine status of adults in Taiwan 2005–2008, 5 years after the cessation of mandatory salt iodization," J. Formos. Med. Assoc., vol. 115, no. 8, pp. 645–651, Aug. 2016.

[34]P. Placidi, L. Gasperini, A. Grassi, M. Cecconi, and A. Scorzoni, "Characterization of Low-Cost Capacitive Soil Moisture Sensors for IoT Networks," Sensors, vol. 20, no. 12, p. 3585, Jun. 2020.

[35]B. Zhou and L. Li, "RETRACTED ARTICLE: Security monitoring for intelligent water-saving precision irrigation system using cloud services in multimedia context," Multimed. Tools Appl., vol. 79, no. 13–14, pp. 9705–9705, Apr. 2020.

[36]K. Taylor and M. Amidy, "Data-driven agriculture for rural smallholdings," J. Spat. Inf. Sci., vol. 20, no. 20, pp. 125–135, Jun. 2020.

[37]X. Chen, H. H. Wang, and B. Tian, "Multidimensional agro-economic model with soft-IoT framework," Soft Comput., vol. 24, no. 16, pp. 12187–12196, Aug. 2020.

[38]A. Kocian, G. Carmassi, F. Cela, L. Incrocci, P. Milazzo, and S. Chessa, "Bayesian Sigmoid-Type Time Series Forecasting with Missing Data for Greenhouse Crops," Sensors, vol. 20, no. 11, p. 3246, Jun. 2020.

[39]I. Mashood Nasir et al., "Deep Learning-based Classification of Fruit Diseases: An Application for Precision Agriculture," Comput. Mater. Contin., vol. 66, no. 2, pp. 1949–1962, 2021.

[40]S. M. Rezvani et al., "IoT-Based Sensor Data Fusion for Determining Optimality Degrees of Microclimate Parameters in Commercial Greenhouse Production of Tomato," Sensors, vol. 20, no. 22, p. 6474, Nov. 2020.

[41]H. Farooq, H. U. R. Rehman, A. Javed, M. Shoukat, and S. Dudely, "A Review on Smart IoT Based Farming," Ann. Emerg. Technol. Comput., vol. 4, no. 3, pp. 17–28, Jul. 2020.

[42]J. Flak, "Technologies for Sustainable Biomass Supply—Overview of Market Offering," Agronomy, vol. 10, no. 6, p. 798, Jun. 2020.

[43]Y. Han, B. Park, and J. Jeong, "A Novel Architecture of Air Pollution Measurement Platform Using 5G and Blockchain for Industrial IoT Applications," Procedia Comput. Sci., vol. 155, no. 2018, pp. 728–733, 2019.

[44]J.-C. Ni, C.-S. Yang, J.-K. Huang, and L. C. Shiu, "Combining Non-Invasive Wearable Device and Intelligent Terminal in HealthCare IoT," Procedia Comput. Sci., vol. 154, pp. 161–166, 2019.

[45]A. Alla and K. Nafil, "Gamification in IoT Application: A Systematic Mapping Study," Procedia Comput. Sci., vol. 151, pp. 455–462, 2019.

[46]J. K. Rogier and N. Mohamudally, "Forecasting Photovoltaic Power Generation via an IoT Network Using Nonlinear Autoregressive Neural Network," Procedia Comput. Sci., vol. 151, no. 2018, pp. 643–650, 2019.

[47]O. Rholam, M. Tabaa, and F. M. et Abbas Dandache, "Smart Device for Multi-band Industrial IoT Communications," Procedia Comput. Sci., vol. 155, pp. 660–665, 2019.

[48]N. Sharma, H. Parveen Sultana, R. Singh, and S. Patil, "Secure Hash Authentication in IoT based Applications," Procedia Comput. Sci., vol. 165, no. 2019, pp. 328–335, 2019.

[49]T. J. Saleem and M. A. Chishti, "Deep Learning for Internet of Things Data Analytics," Procedia Comput. Sci., vol. 163, pp. 381–390, 2019.

[50]D. Oh and J. Han, "Fisheye-Based Smart Control System for Autonomous UAV Operation," Sensors, vol. 20, no. 24, p. 7321, Dec. 2020.

[51]S. Monteleone et al., "Exploring the Adoption of Precision Agriculture for Irrigation in the Context of Agriculture 4.0: The Key Role of Internet of Things," Sensors, vol. 20, no. 24, p. 7091, Dec. 2020.

[52]K. Demestichas, N. Peppes, and T. Alexakis, "Survey on Security Threats in Agricultural IoT and Smart Farming," Sensors, vol. 20, no. 22, p. 6458, Nov. 2020.

[53]K. A. Awan, I. Ud Din, A. Almogren, and H. Almajed, "AgriTrust—A Trust Management Approach for Smart Agriculture in Cloud-based Internet of Agriculture Things," Sensors, vol. 20, no. 21, p. 6174, Oct. 2020.

[54]J. Tian, D. Li, and X. Jia, "IoT Smart Agriculture and Agricultural Product Income Insurance Participant Behavior Based on Fuzzy Neural Network," Comput. Intell. Neurosci., vol. 2022, pp. 1–12, May 2022.

[55]X. Geng and O. Chun, "Multiscale Layout and Planning of Smart Gardens in the Environment of Agricultural Internet of Things," Comput. Intell. Neurosci., vol. 2022, pp. 1–12, Apr. 2022.

[56]B. P. Banerjee, G. Spangenberg, and S. Kant, "CBM: An IoT Enabled LiDAR Sensor for In-Field Crop Height and Biomass Measurements," Biosensors, vol. 12, no. 1, p. 16, Dec. 2021.

[57]Z. Chen, Z. Liao, D. Qian, and J. Li, "Design and Analysis of Intelligent Agricultural Monitoring System Based on Biological Intelligence Optimization Algorithm," Math. Probl. Eng., vol. 2022, pp. 1–8, Jun. 2022.

[58]A. Rehman, T. Saba, M. Kashif, S. M. Fati, S. A. Bahaj, and H. Chaudhry, "A Revisit of Internet of Things Technologies for Monitoring and Control Strategies in Smart Agriculture," Agronomy, vol. 12, no. 1, p. 127, Jan. 2022.

[59]X. Kong, Z. Meng, N. Nojiri, Y. Iwahori, L. Meng, and H. Tomiyama, "A HOG-SVM Based Fall Detection IoT System for Elderly Persons Using Deep Sensor," Procedia Comput. Sci., vol. 147, pp. 276–282, 2019.

[60]M. Yang, "Smart metal forming with digital process and IoT," Int. J. Light. Mater. Manuf., vol. 1, no. 4, pp. 207–214, Dec. 2018.

[61]A. van der Zeeuw, A. J. A. M. van Deursen, and G. Jansen, "How to apply IoT skills at home: Inequalities in cultural repertoires and its interdependency chains," Poetics, vol. 83, no. August, p. 101486, Dec. 2020.

[62]J.-P. Sandvik, K. Franke, H. Abie, and A. Årnes, "Coffee forensics — Reconstructing data in IoT devices running Contiki OS," Forensic Sci. Int. Digit. Investig., vol. 37, p. 301188, Jul. 2021.

[63]K. Y. Najmi, M. A. AlZain, M. Masud, N. Z. Jhanjhi, J. Al-Amri, and M. Baz, "A survey on security threats and countermeasures in IoT to achieve users confidentiality and reliability," Mater. Today Proc., vol. 81, no. xxxx, pp. 377–382, 2023.

[64]J. S. Botero-Valencia, J. Valencia-Aguirre, and D. Durmus, "A low-cost IoT multi-spectral acquisition device," HardwareX, vol. 9, p. e00173, Apr. 2021.

[65]M. Elmoulat, O. Debauche, S. Mahmoudi, S. A. Mahmoudi, P. Manneback, and F. Lebeau, "Edge Computing and Artificial Intelligence for Landslides Monitoring," Procedia Comput. Sci., vol. 177, pp. 480–487, 2020.

[66]I. Izonin, R. Tkachenko, N. Kryvinska, K. Zub, O. Mishchuk, and T. Lisovych, "Recovery of Incomplete IoT Sensed Data using High-Performance Extended-Input Neural-Like Structure," Procedia Comput. Sci., vol. 160, pp. 521–526, 2019.

[67]J. Abijaude, P. Sobreira, L. Santiago, and F. Greve, "Improving Data Security with Blockchain and Internet of Things in the Gourmet Cocoa Bean Fermentation Process," Sensors, vol. 22, no. 8, p. 3029, Apr. 2022.

[68]T. Ando, "Toward the Next Generation of HS-AFM," in NanoScience and Technology, 2022, pp. 107–120.

[69]T. Qayyum, Z. Trabelsi, A. Malik, and K. Hayawi, "Trajectory Design for UAV-Based Data Collection Using Clustering Model in Smart Farming," Sensors, vol. 22, no. 1, p. 37, Dec. 2021.

[70]B. Hassan et al., "A Cost Effective Identity-Based Authentication Scheme for Internet of Things-Enabled Agriculture," Wirel. Commun. Mob. Comput., vol. 2022, pp. 1–12, Apr. 2022.

[71]P. Zhen, Y. Han, A. Dong, and J. Yu, "CareEdge: A Lightweight Edge Intelligence Framework for ECG-Based Heartbeat Detection," Procedia Comput. Sci., vol. 187, pp. 329–334, 2021.

[72]H.-L. Truong, "Using IoTCloudSamples as a software framework for simulations of edge computing scenarios," Internet of Things, vol. 14, p. 100383, Jun. 2021.

[73]M. Javaid, A. Haleem, R. P. Singh, S. Rab, and R. Suman, "Internet of Behaviours (IoB) and its role in customer services," Sensors Int., vol. 2, no. July, p. 100122, 2021.

[74]A. Vij, S. Vijendra, A. Jain, S. Bajaj, A. Bassi, and A. Sharma, "IoT and Machine Learning Approaches for Automation of Farm Irrigation System," Procedia Comput. Sci., vol. 167, no. 2019, pp. 1250–1257, 2020.

[75]Y. Shen, "Information Monitoring of Animal Husbandry Industry Based on the Internet of Things and Wireless Communication System," Comput. Math. Methods Med., vol. 2022, pp. 1–12, Mar. 2022.

[76]V. Meshram and K. Patil, “Border-Square net: a robust multi-grade fruit classification in IoT smart agriculture using feature extraction based Deep Maxout network,” Multimed. Tools Appl., vol. 81, no. 28, pp. 40709–40735, Nov. 2022.

[77]R. Dhaya and R. Kanthavel, “Energy Efficient Resource Allocation Algorithm for Agriculture IoT,” Wirel. Pers. Commun., vol. 125, no. 2, pp. 1361–1383, Jul. 2022.

[78]B. Luo, “A Method for Enterprise Network Innovation Performance Management Based on Deep Learning and Internet of Things,” Math. Probl. Eng., vol. 2022, pp. 1–9, Mar. 2022.

[79]A. Gupta and P. Nahar, “Classification and yield prediction in smart agriculture system using IoT,” J. Ambient Intell. Humaniz. Comput., vol. 14, no. 8, pp. 10235–10244, Aug. 2023.

[80]E. I. Bulatova and E. F. Amirova, “Financial Impact of Digital Technologies as a Promising Element of Import Substitution,” Int. J. Financ. Res., vol. 11, no. 5, p. 392, Sep. 2020.

[81]L. Romeo, A. Petitti, R. Marani, and A. Milella, “Internet of Robotic Things in Smart Domains: Applications and Challenges,” Sensors, vol. 20, no. 12, p. 3355, Jun. 2020.

[82]S. H. Awan et al., “BlockChain with IoT, an Emergent Routing Scheme for Smart Agriculture,” Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 4, pp. 420–429, 2020.

[83]M. Shakeri, A. Sadeghi-Niaraki, S.-M. Choi, and S. M. R. Islam, “Performance Analysis of IoT-Based Health and Environment WSN Deployment,” Sensors, vol. 20, no. 20, p. 5923, Oct. 2020.

[84]C. Li and B. Niu, “Design of smart agriculture based on big data and Internet of things,” Int. J. Distrib. Sens. Networks, vol. 16, no. 5, p. 155014772091706, May 2020.

[85]Y. Rao, M. Jiang, W. Wang, W. Zhang, and R. Wang, “On-farm welfare monitoring system for goats based on Internet of Things and machine learning,” Int. J. Distrib. Sens. Networks, vol. 16, no. 7, p. 155014772094403, Jul. 2020.