Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 7, 5707-5716

Privacy And Security Issues Of Iot In Cloud Computing

Danny Velasco Silva [1], Lourdes Emperatriz Paredes Castelo[2], Milton Paul López Ramos[3], Juan Carlos Santillán-Lima[4]

[1]Facultad de Ingeniería, Universidad Nacional de Chimborazo, Riobamba, Ecuador.
[2]Facultad de Ciencias, Escuela Superior Politécnica de Chimborazo - (ESPOCH), Riobamba, Ecuador.
[3]Facultad de Ingeniería, Universidad Nacional de Chimborazo, Riobamba, Ecuador.
[4]Universidad Nacional de La Plata (UNLP), Facultad de Informática,
Doctorado en Ciencias Informáticas, Calle 50 y 120, CC 1900, La Plata, Argentina.
Email: [1]dvelasco@unach.edu.ec, [2]lparedes@espoch.edu.ec, [3]milton.lopez@unach.edu.ec,
[4]juancarlos.santillanl@info.unlp.edu.ar

Abstract

The technological maturity reached in our days allows electronic devices to connect through the Internet to help the development of almost any activity of human endeavor, thus simplifying our lives. A primary axis for this to happen is an advanced technology that allows the interaction of material objects with a data network, through the use of RFID Radio Frequency Identification (Radio Frequency Identification) sensors. The technology on which this work focuses is the so-called IoT (Internet of Things), together with cloud computing. The combination of these technologies has driven and given a new approach to the lives of human beings since it has allowed them to use in their maximum performance the ubiquitous, communicative, and storage properties of the computer world in which human beings operate. Unfortunately, when users such as IoT devices share network and cloud computing resources, security issues arise. This highlights the need and importance of establishing and respecting policies that ensure the integrity, availability, and confidentiality of data in this shared network environment. The work presented focuses on this critical risk, that is, on the problems of security and data privacy, by analyzing the security problems and challenges that have not yet been solved and that keep researchers in the area of computer security busy. Globally, occupation is justified as these technologies are the future; therefore, they are not receiving more attention in terms of safety. Therefore, it requires the implementation of policies that promote high-level security to ensure data confidentiality, through device authentication, proper management and control of access points, and data network integrity.

Keywords: Internet of Things IoT, RFID, CLOUD computing, network, security, DDoS, vulnerabilities.

I. INTRODUCTION

IoT technology allows various electronic devices to interconnect and interact through the Internet infrastructure. This connection makes it easy for these devices to collect data and share it for different purposes. The power of this great innovation came when these devices were given some digital "intelligence" by mounting sensors and other devices that allowed a real-time response. In the beginnings of this technology, for example, a vending machine was connected through the Internet, but it was not efficient since on the one hand, there was a lack of broadband connectivity and on the other, the chips of that first era of IoT were large and made the connections Complex. The Internet of Things began in 1999 with Kevin Ashton, and this technology took a decade to reach a milestone (Teicher, 2018). Having this technology as we

know it today has been possible thanks to the availability of broadband connections, the cellular network is wireless, with miniaturized chips, and RFID tags, among other technological advances (hardware and software). The system of tags called RFID is used by humans to track the location of objects and/or living beings, in addition, the adoption of IPv6 (Internet Protocol version 6) has made it possible for the IoT to expand its field of action and coverage, since, With its IPv6 implementation, it allows an extremely large number of T devices to obtain IP addresses to communicate on the Internet (Gabbai & Ashton, 2015). This technology was initially used in machine-to-machine communication, but gradually took a strong foothold in the home, smartwatches, and industries, IoT is growing more and more and according to certain predictions, it is estimated that 41.6 billion devices will be connected to the Internet by 2025 (Framingham, 2019). . These are some of the benefits of this technology, but there is also an area of latent concern about it and that is that when using this technology without appropriate security measures, there is a risk of leakage of sensitive and private data of users, with the damages that this causes.

It is important to mention that the F-secure agency analyzed and determined that 300% of cyber-attacks occurred on IoT devices in 2019 (F-secure, 2020). The focus of the study is system-wide attacks and vulnerabilities that occur with this technology. Case studies on the background of technology and the challenges facing technology are discussed. It is also worth mentioning that many companies are migrating their services to the cloud both to mitigate security problems and to improve their hardware resource requirements, this fact has caused many platform providers such as Azure, Aws, IBM, Oracle, etc. are now available (Molina,2022b).

The basic objective of the Internet of Things is to interconnect and integrate the physical world into cyberspace. This integration represents the future demand that will lead to the revolution of the Information Technology (IT) industry(Santillán, 2021). The proposed work presents the background and basic concepts that underpin IoT and its applications. Some important privacy and security concerns that persist over time are also considered. Then, all the cloud provider's services aimed at mitigating risks and building a highly secure cloud platform are mentioned.

II. INTERNET OF THINGS (IOT) APPLICATIONS

Today, many applications employ IoT. The technological maturity reached by highly specialized devices allows human beings to carry out their activities automatically and remotely with the support of Internet infrastructure and services. The Internet of Things is used, for example, to monitor the functionalities of the human body, an area in which this technology is in great demand. Another important application of IoT that facilitates the lives of human beings is the possibility of implementing the so-called "smart home" (or Smart Home), a function with which it is possible to track electronic devices or s as they are called smart devices (Alexa, Google Nest, Sonos One, Apple HomePod, etc.), kitchens, refrigerators and air conditioners in the home, among others. Nowadays it is possible to track the objects in terms of, for example, optimal operating times and temperatures, tasks that have been solved by applying sensors on the objects of interest.

Another no less important application is the tracking of animals, in this case, in the body a GPS transmitter (Global Positioning System) is installed, so that, by detecting the position in real-time, information is obtained that helps in different purposes such for example food. Currently, electronic devices are available that are attached directly to an article to collect various information about it. These instruments detect and send information from different sensors, such information can be for example the temperature, position, and movement of the object, among others. The sensors mounted on an object then make it possible to obtain and transmit information regarding that object in real time, that information is used in decision-making.

IoT applications are structured following an adequate design criterion that has allowed the

reduction of cost and weight, making the hardware necessary to implement this technology accessible and compact. In addition to what has been said, there are IoT applications that are used in other important domains such as health care, smart home, animal care, intelligent transport, and automatic network management (bridges, roads and railways), manufacturing (industry 4.0), smart agriculture, etc(Lima,2021). A personal introspection on how human beings use the Internet of Things is enough to understand this technological trend and validate its purposes. It is also important to consider the domain of your application, the communication technology you use, the size and coverage of the data network, and the bandwidth used, among other aspects that improve the performance of the services supported by this type of technology.

III. LITERATURE REVIEW

The paradigm of Computer Science known as Cloud Computing allows to offer services between an online computer system and the user in three modes: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Examples of such services include operating systems, storage, and cloud servers offered by cloud service providers at affordable prices and with minimal maintenance costs(Molina,2022). These features give the development team the freedom to innovate new technologies to improve since the cloud service provider must provide scalability, agility, elasticity, high performance, and a reliable environment to its customers, thus ensuring the adaptation of the contracted hardware and software infrastructure so that it adapts to the needs and requirements of organizations (Laukkarinen et al., 2013). In this context, one of the challenges that arise when the cloud is used to deliver IoT services is the appropriate allocation of resources, in this case, the cloud service provider solves this problem by matching all its maintenance and performance metrics with the constraints. established in the service level agreement (SLA, for the English Service Level Agreement) (Choi & Lim, 2016).

It is worth mentioning that, in terms of resource allocation, the main factors affecting performance are three: QoS (Quality of Service), user benefits, and resource utilization. The correct establishment of the SLA is then important for both users and cloud service providers before the provider provides its services since the SLA is a legal contract between the two parties, which is measured based on compliance with the metrics offered by the service provider(Lozada,2019). If there is then any failure in terms of latency, security, performance, and consistency offered, a penalty is imposed.

It is normal that in this type of scenario there is a deficit in storage capacity (local) when many sensor nodes are connected to the network, with the use of cloud computing, the sensors connect to the network and send through it the information they collect in real-time, This accelerates the processing of the collected data, this is possible thanks to the use of the high bandwidth and high processing power of the cloud infrastructure that is currently available, which allow the proper linking between the cloud gateway and the gateway of the sensors used. (Yuriyama & Kushida, 2010), RFID systems have benefited from the databases generated with cloud computing since the maturity of the technologies involved allows thousands of labels to be consulted at the same time. This shows that cloud computing and the world of the Internet of Things (IoT), together offer the user different facilities at an affordable cost, a fact that makes it possible to rent services of this type in the cloud, for the use of applications of IoT (Dong et al., 2018). To provide a secure connection between the sensor network and the cloud database, a VPN Virtual Private Network (Virtual Private Network) must be used to maintain a reliable route, this service can be offered by the cloud service provider or by third parties. This helps to safely use the features of cloud computing, among which we can mention: the pay-as-you-go model, server virtualization, the "smart" home, or the multi-tenant lease model that is known to positively

impact the cost of cloud services (Singh et al., 2019).

IV. ELEMENTS OF THE INTERNET OF THINGS (IOT)

Identity. The identity of each device is important as proper identification (each object must have a unique IP address) of the objects on the network allows communication within the network. This identifier can be found in different categories, i.e., each object, communication, and application must have an appropriate identifier. For example, to identify addressing and communication functions, specific identifiers created from real or virtual objects, such as radio frequency and barcoding, are used. Many communications identifiers can accomplish this for communication purposes, using the individual network addresses that each object that integrates the data network must possess. For example, to detect service layers related to applications and logical identifiers, so-called application IDs are usually implemented, a common example of an application identifier is a unique identifier URI (Uniform Resource Identifier) or URL (Uniform Resource Locator). There are a large number of IoT platforms that coexist in the network, this fact as expected leads to interoperability between the networks involved themselves interacting to assign objects as identifiers that are included in the identification scheme. The Electronic Product Code (EPC), used to uniquely identify any object and which replaces the barcode, for example, specifically defines an object that is equipped with an RFID tag. Ubiquitous codes and Epronic E-codes of Products (EPCs) are used to assign naming functions to the object (Burhan et al., 2018).

Detection. Detection is a function that is responsible for collecting information from an object, and this process is done in real-time. This information is stored on the storage media used. Actuators of this type are for example RFID tags, the so-called "smart" sensors, portable detection devices, and among others, these actuators are the devices that from a series of sensors can collect information required of an object. Table 1 presents the key elements and technologies of the Internet of Things (IoT).

Communication. The Internet of Things provides connectivity, therefore, one of its functions is the interconnection of several systems. This communication makes it possible for different devices and/or objects to send and receive messages, files, and other data. This communication is possible thanks to the use of radio frequency identification (RFID), Near Field Communication (NFC), Bluetooth, and Wi-Fi among other technologies.

Computation. This is a method based on the processing of information collected from objects equipped with sensors. This process is served, among other things, to eliminate unwanted or irrelevant information that is not required for the decision-making process(Molina,2022a). This method uses a set of software tools and other resources that accelerate the operation of the Internet of Things. In this sense, the operating system is an engine for the platforms related to the application, and the platform related to the equipment that is used (Audrino, Raspberry Pi, etc.), plays an important role in the way in which the actions are carried out. It uses a variety of operating systems such as Tiny OS, Lite OS, Android, etc.

Services. Internet of Things applications generate 4 steps of services. The first service is identification, this service allows one to identify an object, the aggregation of information is another service that allows collecting information from objects of interest, The third service is the processing of the information collected, which allows one to decide it, the fourth service is ubiquitous and transparent to the user, it runs instantly without the rigidity of time and position to update to the devices.

Semantics. Semantics ensures that Internet of Things devices interoperates despite belonging to different providers. It is a very important element of this technology since from the information received, it tries to act like the human brain (based on Artificial Intelligence and Machine Learning processes), and makes rational decisions.

Table 1: IoT Elements and Related Technologies

IoT element	Technology
Identification	IPv4, IPv6, Electronic Product Code, Ucode.
Detection	RFID Tags, Sensors, Actuators, and Portable Sensing Devices.
Communication	Radiofrequency identification, Wireless sensor networks, Near field communications, Bluetooth.
Computation	Raspberry Pi, Arduino, Intel Galileo.
Services	Related Identity, Information Aggregation, Ubiquity, Collaborative Awareness.
Semantics	RDF (Resource Description Framework), Web Ontology Language (WEB

Source: The authors

V. METHODOLOGY

The basic design of the Internet of Things covers 4 pillars, which are: Perception, Application, Red, and Processing (Suchitra & Vandana, 2016), cited by (Omolara et al., 2022). Figure 1 shows the IoT architecture.

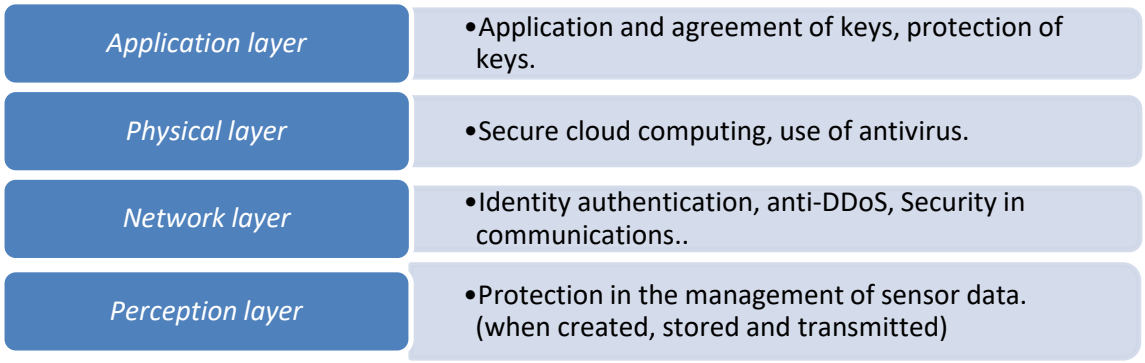

Figure 1: Internet of Things architecture
Source: The authors (Suchitra & Vandana, 2016) and (Rojas et al., 2022)

Description of the 4-layer IoT architecture:

1) Perception layer. This layer is responsible for the recognition and consists of several sensors that work with various technologies such as infrared, RFID, ZigBee, and QR code. This layer collects and collects information related to the device and its environment, the data can be referring to temperature, pH level, humidity, pressure, etc. This stage of IoT handles important parameters, such as tangible components and network connectivity applications, these elements are important as they determine how information collected and collected in the Internet of Things is collected and transmitted ranging from the sensors involved to the other layers of the model.

2) Network layer. This layer acts as a brain by serving as a bridge between its 2 adjacent layers. In this stage of IoT, the secure transmission of the information collected is guaranteed, this transmission is carried out through network infrastructures such as the Internet, communications networks, mobile and wireless networks, etc. It should be noted that for

communication purposes, the exchange of collected information occurs between devices through these networks.

3) Physical layer. This layer creates a secure support structure for the application layer; this support is responsible for organizing the required computational capacities with the use of a network cluster. This enables the fusion and proper functioning of IoT applications.

4) Application layer. This is the terminal layer, in which IoT users have personalized services according to their requests and requirements. It is at this level that, through various customized devices (computers and others), users have a friendly and usable interface that makes it possible to access Internet applications.

VI. ANALYSIS OF VARIOUS ATTACKS IN IOT

1) Incorrect API Gateway configuration. As expected, communicating with an IoT cloud server efficiently and quickly is desirable and good practice for performance issues. This is important for IoT devices to use an Application Programming Interface (API) interface as a gateway to request certain actions to be executed on the cloud server (Darwish et al., 2013) , cited in (Aydın et al., 2022). The aforementioned interface provides good link support due to the functions implemented in it, for example, you can not miss a proxy or a firewall well configured to restrict unwanted traffic and avoid possible bottlenecks in the network (Lozada,2021). This fact improves the performance of IoT since it allows the change and adaptability of the device according to its requirement, through the examination of the state of the device, and actions that are executed transparently to the user.

Therefore, if this type of crucial device is misconfigured, the data network is compromised and vulnerable to attacks of various types, which shows that there must be an important responsibility in aspects of computer security. Most computer attackers take advantage of this vulnerability and can exploit it to execute attacks such as unauthorized password changes, execution of malicious code, penetration attacks, user forgery, spoofing, man-in-the-middle attacks, denial of services, etc.

2) Failure to comply with established security roles, policies, or keys. It is common for developers to customize roles and policies for proper cloud connectivity. Usually, the process inherent in the use is done and, during this process, each system must handle a workload that, as already mentioned, corresponds to a security responsibility that must be considered to safeguard the data. To simplify this configuration, many vendors use the same design for the IoT device, creating significant problems (Paucar,2022). However, it is important to mention that incorrect configuration of Identity and Access Management (IAM) can not block or hinder data traffic and that this would make it possible for a malicious person (hackers), to perform some type of attack on the cloud server, who could even perform more targeted attacks that allow them to monitor the cloud service by posing as a legal user of devices with access to IoT services (Bokefode et al., 2016).

3) Vulnerabilities in devices, communication channels, and infrastructure. As already mentioned, APIs frequently use to perform automatic transmission and connectivity from different service providers, which are known as API gateways. In that sense, both the Internet of Things infrastructure and the cloud server use a common gateway to communicate the cloud server infrastructure with IoT devices. This configuration ends in configuration errors that can trigger attacks on devices. Apart from what has been said about devices and gateways in the cloud, it is worth mentioning that, the network infrastructure can detect the fragility in the security of data traffic and several open-source platforms are available to fulfill this task through network health checks.

4) Denial of Service (DDoS) attacks. IoT devices are the main target of this type of attack, which is executed through the HTTP protocol (HTTP must be used), statistics indicate that this attack continues to grow. Usually, behind this attack is a botnet configured to leave the network out of service, being a trend, the use of the Web

Services for Devices protocol WSD (the English Web Services for Devices) to discover and contact nearby devices and in this way, amplify the effect of DDoS attacks (Ravichandran, 2017). The problem with WSD servers is that they respond to unauthenticated requests, providing an opportunity for computer attackers or hackers.

VII. RESULTS

The paradigm of cloud computing involves a group of virtualized and connected servers working in cluster mode to increase their computing and storage potential compared to a desktop computer. The cloud infrastructure then executes different applications and services that support the operation of an Internet of Things environment, said infrastructure turns out to be highly efficient to perform the analysis of data that are collected by IoT sensors, such analyzes allow the taking of Correct decisions from different devices and sensors.

It turns out that the Internet of Things can be a double-edged sword, since, although it provides greater connectivity, if it is poorly designed and/or configured, it will also put the entire system in vulnerable conditions. In this sense, it is recommended that the collected information that transits through the network is encrypted and that such data is stored in the cloud using secure keys that must be protected when created, stored, and even more so when shared (Chopkar et al., 2014).

To design and implement a secure, scalable, reliable computer system and control access to the network, the network administrator must form groups of users within which they are assigned to the levels according to their roles and permissions, also respecting certain standard conditions according to those roles. The responsibility for the application of this type of action is assumed by the Administrator, a member of the IT department who will provide permissions and access rights to users according to each assigned role and who can also eliminate the roles assigned to each user or group of users. The storage of data must also consider some metrics that ensure the integrity of the data, without neglecting its confidentiality and availability in that sense cloud service providers must ensure that information (whether IoT or not), is stored in a coded and encrypted structure so that not even the Service provider can view or read this data, and that it is accessible only by authorized persons, users of cloud services.

If each local account or application is migrated to the cloud, security must be provided on the cloud service provider's server, being responsible for implementing an additional layer of security based for example on the JavaScript Object Notation JSON (JavaScript Object Notation). All incoming and outgoing network traffic must pass through the API gateway following established security processes, greatly reducing the possibility of attacks occurring.

One of the important points is undoubtedly the understanding and application of a model of shared responsibility existing between the customer of IoT services and the cloud service provider. As an example, in the Amazon AWS Web Services (Amazon Web Services) shared responsibility model, all hardware components are the responsibility of the vendor. According to the requirements of the application, the customer maintains the type of operating system, the type of storage, and the configuration. In working environments with multiple clouds, devices and their connectivity can be more than complex, a fact that can lead to undesirable data leakage, credential leakage, or generate vulnerability in the data network. It is important to have a clear knowledge of the network infrastructure to understand how it works and thus keep track of the changes that may occur in the network infrastructure. This will enable network administrators to be prepared to take appropriate actions on the devices to protect them from different types of attacks.

Anyone who prides himself on being a cloud service provider will add a service that allows monitoring traffic and detects, among other things, anonymous activity. This service works as a firewall to prevent the application and network from being attacked. Most attacks occur in IaaS and PaaS service delivery modes, so implementing this type of security service provides an extra layer of protection to

resources. This service can be applied to resources such as DNS servers, devices, and elastic load balancers.

As for information storage, cloud storage must ensure a secure and reliable online store that serves many users at the same time. Current cloud security systems rely on identifying when someone tries to enter the system or in case some malicious activity occurs. The implementation of multiple levels of detection in the System, for example, IDS Intrusion Detection System (IDS), provided by cloud service providers, can largely prevent intruders from breaking through the initial network defenses and executing your attacks.

VIII. CONCLUSIONS

The rapid development of Internet-based computing has allowed the development of many technologies to meet the growing demand. This shows the need to recognize the vulnerability of this type of technology, it is, therefore, important to consider mechanisms and techniques that guarantee the protection and privacy of information in IoT environments. The growth of the Internet of Things is enormous so there are persistent and new challenges and difficulties that must be addressed by the research community in the area.

The Internet of Things is perceived as new and disruptive technology. In the work presented, the focus has been on various types of network attacks that can occur in the IoT environment and on the actions that are being applied to security and privacy issues. In addition, the importance of secure storage of information in the cloud is evident, in which encryption methods must be applied. Depending on the case, you can aggregate, for example, the critical data of the organization in a private cloud and other data in the public cloud. The current practices applied to this process, make the IoT environment in the cloud secure and, simultaneously, through the cloud service provider it is possible to apply cryptographic techniques such as RSA or AES, to ensure the secure transport of data. In addition, it is possible and highly recommended to assign roles and permissions to each user, being able to block their access if necessary. These actions make it possible to build a high-level security wall for the system.

The application of solutions related to the improvement of security in IoT environments (such as privacy, trust, identification, and access control), the proper determination of security policy and compliance, as well as the standardization of the network facilities of the organization with the facilities of the cloud service provider, among other measures, allow better control of the network against the great risk that exists in this type of shared infrastructure.

REFERENCES

1. Aydın, H., Orman, Z., & Aydın, M. A. (2022). A long-term memory-based distributed denial of service (DDoS) detection and defense system design in a public cloud network environment. Computers & Security, 118, 102725. https://doi.org/10.1016/j.cose.2022.102725
2. Bokefode, J. D., Bhise, A. S., Satarkar, P. A. & Modani, D. G. (2016). Development of a secure cloud storage system to store IoT data by applying role-based encryption. Procedia Computer Science, 89, 43-50. https://doi.org/10.1016/j.procs.2016.06.007
3. Burhan, M., Rehman, R. A., Khan, B., & Kim, B.-S. (2018). IoT Elements, Layered Architectures, and Security Issues: A Comprehensive Survey. Sensors, 18(9), Art. 9. https://doi.org/10.3390/s18092796
4. Choi, Y. & Lim, Y. (2016). Optimization approach for resource allocation in Cloud Computing for IoT. International Journal of Distributed Sensor Networks, 12(3), 3479247. https://doi.org/10.1155/2016/3479247
5. Chopkar, S. K., Chakrabarty, D. K., Gangakhedkar, K. R., Dhone, A. B., Chopkar, P. S., Vakharia, J. J., & Kharate, R. M. (2014). Condensation and formation of water droplets due to

endothermic reaction by laser pulse through natural lighting phenomena in the atmosphere. International Journal of Management Studies and Research (IJMSR), 2(10), 148-155.

6. Darwish, M., Ouda, A. & Capretz, L. F. (2013). DDoS attacks and cloud-based defenses. International Conference on the Information Society (i-Society 2013), 67-71.
7. Dong, Q., Chen, M., Li, L., & Fan, K. (2018). Cloud-based radio frequency ID authentication protocol with location privacy protection. International Journal of Distributed Sensor Networks, 14(1), 1550147718754969. https://doi.org/10.1177/1550147718754969
8. Framingham, M. (2019, June 18). The growth of connected IoT devices. https://www.businesswire.com/news/home/20190618005012/en/The-Growth-in-Connected-IoT-Devices-is-Expected-to-Generate-79.4ZB-of-Data-in-2025-According-to-a-New-IDC-Forecast
9. F-secure. (2020). Useful articles and tips on online safety. https://www.f-secure.com/es/home/articles
10. Gabbai, A. & Ashton, K. (2015). He describes "the Internet of Things." http://www.smithsonianmag.com/innovation/kevin-ashton-describes-theinternet-of-things-180953749/#agslvMb1jBsI5te8.99
11. Laukkarinen, T., Suhonen, J., & Hännikäinen, M. (2013). An integrated cloud design for the Internet of Things. International Journal of Distributed Sensor Networks, 9(11), 790130. https://doi.org/10.1155/2013/790130
12. Lozada-Yánez, R., Molina-Granja, F., Lozada-Yánez, P., & Guaiña-Yungan, J. (2020, April). Machine Learning and Data Networks: Perspectives, Feasibility, and Opportunities. In World Conference on Information Systems and Technologies (pp. 275-292). Springer, Cham.
13. Lozada-Yánez, R., Luna-Encalada, W., Tierra-Quispillo, D., Molina-Granja, F., & Guaiña-Yungan, J. (2019, July). Routing protocols in vehicular ad-hoc networks: a performance evaluation. In International Conference on Knowledge Management in Organizations (pp. 477-488). Springer, Cham.
14. Lima, J. S., Molina-Granja, F., Lozada-Yanez, R., Velasco, D., Peñafiel, G. A., & Castelo, L. P. (2021, July). The importance of the digital preservation of data and its application in universities. In International Conference on Knowledge Management in Organizations (pp. 345-353). Springer, Cham.
15. Molina-Granja, F., Granda, W. B., Altamiran, J. D., & Ramos, P. L. (2022). Maturity Model for Data Analytics in Health Institutions. Journal of Positive School Psychology, 4585-4590.
16. Molina-Granja, F., Lozada-Yánez, R., Santacruz-Sulca, F. J., Ramos, M. P. L., Vignesh, G. D., & Swaminathan, J. N. (2022a). Design of Social Distance Monitoring Approach Using Wearable Smart Tags in 5G IoT Environment During Pandemic Conditions. In IOT with Smart Systems (pp. 731-740). Springer, Singapore.
17. Molina-Granja, F., Barba-Maggi, L., Molina-Valdiviezo, L., & Bustamante-Granda, W. (2022b, June). Demand and employability study of the data science engineering career in Ecuador. In 2022 17th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-5). IEEE.
18. Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., Alshoura, W. H., & Arshad, H. (2022). Internet of Things security: a survey covering unexplored areas and new knowledge. Computers & Security, 112, 102494. https://doi.org/10.1016/j.cose.2021.102494

19. Paucar-León, V. J., Molina-Granja, F., Lozada-Yánez, R., & Santillán-Lima, J. C. (2022). Model of Long-Term Preservation of Digital Documents in Institutes of Higher Education. In International Conference on Knowledge Management in Organizations (pp. 257-269). Springer, Cham.
20. Ravichandran, S. (2017). The cloud-connected smart gas cylinder platform detects LPG gas leaks using the IoT app. MC Square International Journal of Scientific Research, 9(1), 324-330.
21. Rojas, C. A., Chanchí, G. E., & Villalba, K. M. (2022). Proposal of an IoT Architecture for the domotic and inmotic control of buildings—ProQuest. https://www.proquest.com/openview/7faf260884f64e41c74f8f94e7172604/1?pq-origsite=gscholar&cbl=1006393
22. Santillán-Lima, J. C., Haro-Parra, P., Luna-Encalada, W., Lozada-Yánez, R., & Molina-Granja, F. (2021, September). Security Techniques in Communications Networks Applied to the Custody of Digital Evidence. In The International Conference on Advances in Emerging Trends and Technologies (pp. 298-309). Springer, Cham.
23. Singh, S., Ra, I.-H., Meng, W., Kaur, M., & Cho, G. H. (2019). SH-BlockCC: A secure and efficient smart home architecture of the Internet of Things based on cloud computing and blockchain technology. International Journal of Distributed Sensor Networks, 15(4), 1550147719844159. https://doi.org/10.1177/1550147719844159
24. Suchitra, C. & Vandana, C. (2016). Internet of Things and security issues. International Journal of Computer Science and Mobile Computing (IJCSMC), 5(1), 133-139.
25. Teicher, J. (2018). The little-known story of the first IoT device. IBM Industries blog. https://www.ibm.com/blogs/industries/little-known-story-first-iot-device
26. Yuriyama, M. & Kushida, T. (2010). Sensor cloud infrastructure: physical management of sensors with virtualized sensors in cloud computing. 2010 13th International Conference on Network-Based Information Systems, 1-8. https://doi.org/10.1109/NBiS.2010.32