ISSN 2007-9737

Cybersecurity and Internet of Things. Outlook for this Decade

Jairo Eduardo Márquez Díaz

Universidad de Cundinamarca,
Colombia

jemarquez@ucundinamarca.edu.co

Abstract. The Internet of Things is one of the technologies with the greatest incursion and expansion in the services market, making it attractive to cyberattacks due to its various vulnerabilities, both in its protocols and in its implementation. This brings with its aspects that the industry and users must take into account to minimize the risk of suffering various types of attacks, compromising sensitive information in the process. In this sense, a study on the advantages and disadvantages of the IoT is shown, focusing on the protection of information based on its present flaws, which will eventually have to be taken into account for future developments that involve data management and administration through devices. smart. The methodology used is based on theoretical and quasi-experimental research represented in the skills and experience in ethical hacking applied to the corporate environment. In this way, the most representative flaws in terms of cybersecurity related to the IoT are exposed, so that they are attended by companies and personnel responsible for their security.

Keywords. Advanced persistent threats, botnet, cyberattacks, distributed denial of services, ransomware.

1 Introduction

The internet of things (IoT) refers to the set of electronic devices connected to the internet that are permanently recording and sharing data. Under this scenario, any electronic device (bioelectronic or nanoelectronic) including household appliances, office equipment, machinery, accessories attached to clothing and personal items that share data among themselves or a central, belong to the world of IoT.

For this new decade, the technology represented in the Internet of Things (IoT) with its various variants such as: Internet of Vehicles (IoV), Internet of energy (IoE), industrial IoT, artificial intelligence in IoT (IAoT), Internet of Things-Grid (IoT-G), Internet of Robotized Things (IoRT), IoT on the Battlefield (IoTotBF) [1], Internet of Wearables Things (IoWT), Internet of Medical Things (IoMT), etc., van to set the pace of societies in various contexts, whose objective will be framed in improving the quality of life of people, industry, cities and the environment through increased connectivity, navigability, monitoring, interaction and ubiquity, either in an environment urban as rural.

This brings with its new challenges in terms of security and regulations that not only guarantee the proper use of technologies, but also the algorithms that control them, in this particular case artificial intelligence (AI) through developments based on deep learning and machine learning [2].

The demand for new technologies, applications and IoT solutions in this new decade will be marked by digital health care and control, as well as the development of intelligent environments (which involve the labor field, recreation, transportation, home and study among others) that allow remote monitoring of any variable that implies improving a service in favor of people's well-being.

This requires high-speed network technologies equipped with new connectivity protocols that guarantee a higher speed rate than the current one, with low latency and protection against cyberattacks.

In addition to the above, connectivity will not only be represented in 5G, WiFi (including its latest variants such as WiFi 6) or LiFi technologies, but also in low-orbit satellite communication.

This represents a challenge, based on the fact that the space around the Earth is being increasingly saturated with satellites, which is why the market for services is expected to increase for this decade.

For example, the Starlink company with its plan to have 12,000 satellites, provides high-speed connectivity services worldwide with its scarce 1,000 satellites at the time of writing this article, in addition to other satellite fleets from several countries that intend to expand this service by placing hundreds of thousands of these artifacts into orbit.

With this in mind, it is clear that the societies of the 21st century are going to be permanently connected anywhere in the world, with multiple services according to the needs of each user and industry. Although it should be noted that this connectivity may be expanded to other worlds before half a century, such as the Moon and Mars, as planned by large aerospace industries.

2 Internet of Things and Vulnerabilities

The IoT is increasingly present in our daily lives, either at home or at work, being essential for monitoring variables such as temperature, humidity, flow rate, pressure, electrical conductivity, pH, measurement of heavy metals. in the air, access control, security, driving, purchase of items, vital signs, active biological pollutants, etc., all using the wireless internet as a means of communication.

This implies that the IoT presents specific functions for capturing data from the environment, which are then processed and stored to later analyze the convergent information for decision-making. This process demands the use of distributed networks adjusted to universal standards as those of each manufacturer, for which the devices make use of sensors and / or actuators in order to communicate with each other.

Another aspect to take into account about the IoT is that it is constantly evolving, with a moderate bandwidth demand that promises to increase with the incorporation of machine learning algorithms, expanding its services, giving way to the so-called Analytics on the Edge [3].

Also, the IoT being scalable allows several of its data capture and recording processes to be optimized; This affects the use of energy efficiently (remembering that they are wireless devices that work with batteries).In the same way, the IoT uses modern Web technologies for its connectivity and data transfer in real time, either to a local server or a central one in the cloud (servers/platform), so that its applications are extended to different fields using multiplatform mobile applications on a recurring basis.

Regarding the wireless connectivity of IoT devices, it is carried out through wide coverage networks such as LPWAN that include Sigfox, LORA and NB-IoT networks, where each one is characterized by working under different modulations and bandwidths. according to the own needs on which they work in each country [4].

At the security level, there is a great diversity of problems that IoT technology presents in terms of manipulating its operating environment, either through hardware or software, as summarized below:

1 Vulnerable wired and wireless network services due to factors such as: weak passwords that allow easy cracking, insecure password recovery systems, buffer overflow, outdated firmware with active back doors, API (*application programming interface*) problems in the devices and backend of manufacturers and third parties, DoS, DDoS, account locks and credential management, malware injection and replay and brute force attacks, unencrypted or improperly encrypted services, weaknesses in UDP services and protocols of UPnP (*Universal Plug and Play*) communication, inadequate payload verification and message integrity among many others.
2 Human factor: other weaknesses are attributed to the updating and authentication mechanisms whose responsibility on the part of the network administrator is critical. In this sense, failures are detected in updates that do not appear encrypted or with write permissions, or authentication is not enabled for firmware and patches, etc.
3 In the framework of authentication, there are variants that many administrators take as one.

For example, between IoT device to device, IoT device to mobile application, IoT device to cloud, mobile application to cloud, and web application to cloud. With any failure in any of these authentications, the entire network is compromised in terms of its privacy, being exposed to disclose the location and data of the user(s).

Now, as the IoT is in continuous expansion in the services market, it has also demonstrated its importance in the social, health and industrial framework, especially when there are already strong synergies with disciplines such as Big Data, artificial intelligence (AI), Cloud computing, artificial vision as a service (CVaaS), Edge computing, perimeter computing and blockchain among others, which have been laying the foundations for the development and consolidation of technologies such as Smart Systems (which involves Smart energy, Smart home, Smart buildings, Smart Cities, Smart transport, Smart Health, and Smart industry) and the IoT of Wearables (IoWR).

In the same way, the relationship between IoT and AI is growing, being incorporated into various devices, where household appliances are no exception, thus seeking to improve energy efficiency and the security of the data that circulates both through the devices and through the network to which they are connected to the home, building or industry.

Under this scenario, a problem to overcome consists of the incorporation of deep learning programs in the diversity microcontrollers of IoT devices, in particular memory chips, whose capacity is limited, hence the data is currently sent to the cloud that, of course, can be vulnerable to cyberattacks, if certain information security policies are not complied with. An advance in this direction is the TibyNAS algorithm, which as stated [5] "generates compact neural networks with the best possible performance for a given microcontroller, without unnecessary parameters", which is combined with the MCUNet system in charge of image classification locally, thereby reducing the risk of information theft.

This type of advance is crucial for future technologies, based on the fact that the number of household appliances, wearables and IoT devices implemented in people, homes, buildings, industry, transport and cities in general, is growing day by day, which is expected. exceed one billion devices, where limitations such as memory and processing capacity will be quickly overcome; This will demand a large amount of data storage and processing resources, therefore, Big Data in conjunction with disciplines of AI and data engineering will contribute their own in this regard.

3 Vulnerabilities in Protocols

The protocols that govern the IoT have been for many years one of many critical security weaknesses, which have demanded to be addressed in order to guarantee a standardized intra- and inter-device communication that has been partially solved. However, there are non-standardized protocols related to the IoT such as Zigbee, Z-wave, XBee, bluetooth, WiFi and LoRa among others, which work on the open-source stacks of TCP/IP protocols, which in turn present vulnerabilities in each structure since its creation, starting in most cases due to memory corruption. These flaws allow different types of malware, DDoS attacks and DNS record injection to be executed that expose the information to a cyberattack.

It is important to note that the TCP/IP model presents the entire structure on which a set of specific network protocols allows any equipment or nodes to communicate end-to-end, under specific addressing for both transmission-reception and routing between other technical aspects. The vulnerabilities of the TCP/IP protocols are exploited to carry out DDoS-type attacks according to the layer, so [6] classify them as follows:

a. Application: in this layer the most common attacks are: HTTP / HTTPS Flooding, FTP Flooding, Telnet DDoS, Mail Bombs, SQL Slammer and DNS Flood.
b. Transport: the attacks are of a volumetric type, understood in the sense that it is aimed at destroying networks, denying or consuming their resources until the server collapses. The most common DDoS attacks are: SYN Flooding and UDP Flooding and TCP Null Flooding.
c. Internet: attacks occur in this layer due to vulnerabilities inherent to the design of the

TCP/IP protocols. The most common attacks are Smurf (compromises the ICMP protocol), Fraggle, TearDrop and ICMP Flooding.

d. Access: Attacks exploit weaknesses in the network layer and its protocols. The most common DDoS attacks are: VLAN hopping, MAC Flooding, DHCP Attack, and ARP Spoofing.

Other vulnerabilities directly related to IoT systems are open-source TCP/IP stacks, which are not owned by a single company, these are: PicoTCP, uIP, FNET and Nut / Net, which are present in IPv6 protocols, DNS, mDNS, TCP, ICMP and LLMNR, all of them related to the communication of devices connected to the internet. A particular example related to TCP are DDoS attacks through Microsoft's Remote Desktop Protocol (RPD), taking advantage of UDP port 3389; Although a set of privileges is required, this type of attack cannot be ruled out even with patches and possible unauthorized access within a network.

As a complement to the above, there are vulnerabilities inherent to the operating systems and the architecture that the current Internet supports, which are connected to servers, computer equipment, IoT devices, access controls, etc., which is a real problem for the time to know the operational characteristics of the firmware and connectivity hardware of these elements to establish if they are at risk or not, added to the presence of bad practices in software development.

For example, there are online resources, specialized software or a simple script (https://github.com/Forescout/project-memoria-detector) that allow probing the ICMP protocol, TCP option signatures and handling of their flags to detect vulnerabilities and take corrective actions in order to prevent future attacks.

To finish this section, the Thread protocol [7] has recently been proposed, which is supported by the major industries of IoT technology through the Thread Group, designed to establish secure wireless IP connectivity without the need for concentrators or hub thanks to the use of IPv6 and 6LoWPAN standards. The Thread protocol uses encryption mechanisms to guarantee secure communication, even via Bluetooth.

In addition, this protocol guarantees the transparency of connectivity between devices, expanding a network if necessary, taking into account low energy consumption. With this in mind, as IoT devices and coverage increase, the problem of saturation and range of action is resolved respectively, in addition to the fact that the network adapts in case a device fails.

Therefore, it is expected that this protocol will be adopted by the entire industry, minimizing the compatibility problem of IoT technologies present today.

4 Geopolitics and IoT

The COVID-19 pandemic has taught society great lessons and one of them is that you cannot let your guard down in the face of an epidemic that can spread rapidly throughout the world. Mandatory confinement brought to the fore the fragility of the health sector in treating conditions, detecting and treating chronic diseases, due in part to the fact that clinical procedures were planned to be developed in hospital facilities and laboratories.

The IoT proposal based on the above, was to increase the number of devices implemented at home, work and even the patient's body, in such a way that monitoring is carried out in situ, controlling the patient's health status, minimizing risks associated with a disease getting out of control. With this new monitoring perspective, the industry and health companies have begun to massively introduce the IoT in their facilities and homes of workers and patients respectively, seeking to improve their safety and care. In this sense, it seeks to improve the efficiency of the resources used within a company, for example, using intelligent lighting systems, intelligent energy and environmental control, security systems and monitoring in areas of low and high traffic among others, which guarantee the well-being of the worker.

However, although the interest in using the IoT has increased, so has the risk of compromising sensitive information to third parties, due to the vulnerabilities inherent to this technology, added to the geopolitical instabilities that have opened a gap to cybercrime in recent years for carry out attacks of various types.

It is evident that technological ubiquity and dependence on it draws attention to cybercrime, especially under the global economic and geopolitical uncertainty that apparently will remain in this way for some time to come.

Thus, advanced persistent threats (APT) [8], ransonware and DDoS attacks will be the common denominator for the next few years.

These cyberattacks have various connotations: economic, personal, corporate, political and geopolitical, just to name a few. In the particular case of geopolitics, it is marked by new technical and technological innovations that seek that particular target (diplomats, governmental and non-governmental organizations, health centers, research centers, universities, etc.) fall into digital traps, downloading files corrupt or malicious attachments in order to steal and / or hijack your systems.

In the case of cyberattacks directed at government platforms, defense and technology companies and critical infrastructures (understood as: hospitals, transport and energy sectors, roads, bridges, tunnels, airports, seaports, public services, buildings, etc.), they seek control your computer networks through the creation of chains of infection, phishing and use of legitimate services, making it almost impossible to take corrective action in this regard.

The problem with this type of cyberattack is that its source points to Russian, Chinese, Iranian and North Korean organizations (a fairly complete list can be consulted in this regard SINCE 2016 in CSIS) [9]. In this type of scenario, there are other cyber-piracy groups from countries such as Vietnam [10, 11], which, through their social networks, spread all kinds of malware and phishing with political objectives and the interests of the Vietnamese government, for example, property theft. intellectual and cryptocurrency mining. These types of cyberattacks seek the collection of confidential business information that is sold to the competition. The modus operandi is the sending of messages to the holders of emails with directing to false pages, this implies the use of techniques such as social engineering, spear-phishing [12] and pharming [13] among others.

It should be noted that techniques to bypass the security of a physical and logical system are permanently refined, for example, dropping PE (*Portable Executable*) binaries to load advanced malware, combined with basic or low-tech techniques.

The goal is to control the victim's operating system in such a way that it is not easy to reinstall it or even replace the hard drive. Another way to increase the success rate of attacks using phishing-type malware is through the implantation of emails directly to the entrance of the victim's mailbox, using tools such as Email Appeder. With this system, email security is circumvented, because the incoming email credentials are valid, so once approved it connects to the victim's email accounts through the IMAP (*Internet Message Access Protocol*) protocol, which is responsible for receiving messages from a mail server. Once this step is completed, the cybercriminal customizes the messages so that they are credible and the victim accepts them, opens and enters personal or corporate information. The problem with this type of attack is that it is new, with a high degree of effectiveness, so the risk of being attacked under this advanced phishing scheme should not be underestimated, especially in companies and industry in general.

Another type of malware recently discovered, shows the new generation of computer worms that IoT systems and operating systems will have to deal with in the coming years, called Gitpaste-12. This type of malware used GitHub and Pastebin to store the code of its components and host 12 different attack modules to attack different vulnerabilities. With these characteristics, it has the ability to propagate progressively in a corporate network emulating what a botnet would do, but internally, compromising devices such as routers, firmware and operating systems, using exploits, which then proceeded to execute a dynamic script with in order to download and run the other components of Gitpaste-12, which were constantly updated and at the same time disabled the security protocols.

It also includes the rules of firewall devices, software for monitoring and prevention of attacks, the apparmor module (this module belongs to the Linux kernel that allows restricting some processes of certain programs as an administrator) and commands related to access security. Cloud. This implies that this type of threat aims to have access and control of the infrastructure that connects and

manages cloud computing and, therefore, the data of all IoT devices and other connected systems.

To make matters worse for the victim, this worm runs a cryptominer, the objective of which is to hijack the idle processing of the network and extract cryptocurrencies for other fraudulent attacks, either to other external services such as the victim's clients.

This type of attack is perverse, since it not only has access to all the victim's data, but also uses its own infrastructure to attack others, preventing the network administrator from collecting information on those processes that are running by blocking certain instructions, such as: readdir, tcpdump, sudo, openssl, /proc, etc. Finally, the Gitpaste-12 worm at the time of discovery contained a library that downloaded and executed Pastebin files that contained more malicious code.

What this type of malware hints at is that they are sophisticated programs designed to deal with new developments at the security level of operating systems and firmware of devices connected to a network, selectively attacking the IP addresses contained within a network. random range of classless interdomain routing CIDR (classless interdomain routing), execution of scripts to open certain ports such as 30004 related to the Transmission Control Protocol (TCP) and port 30005 related to the bidirectional SOAP / HTTP protocol, in charge communication between router devices or network switches, as well as automatic configuration servers.

In conclusion, the emergence of new worms with botnet characteristics will increase in the coming years (for example, the Golang worm), with the mitigation that they will be combined with other intrusive techniques such as crypto mining to attack servers with Windows operating systems and Linux, cloud systems with exploits that link ransomware, APT and DDoS with all their variants [14].

Governments and industry have begun to take action on the matter, however, not only cybercrime is taking a step forward, but also organizations sponsored by the State itself, contracted to carry out targeted attacks on organizations and industry from other nations [15, 16].

5 Ransomware Attacks

Ransomware is a type of cyberattack characterized by hijacking information from a system by encrypting it, and then charging the victim for its ransom with a fixed term, through payment by means of electronic currency such as bitcoin.

By not acceding to these claims, cybercriminals proceed to delete the information, auction it or publish it on filtering sites on the darknet so that other criminals can appropriate it and thereby perpetuate the scam. A recent method of pressuring the victim to pay when she refuses is by harassing and coercing her through intimidation that ranges from disclosing exfiltrated information to threatening the lives of employees and their families. This cyberattack panorama has shown a constant evolution in the last decade, both in the form of attack and in the means of pressure exerted by the payment to release the release, as evidenced by the most known ransomware-type malware worldwide such as They are: Wannacry, Bad rabbit, Peya, Spora, Reveton, Doxware, Locky, Zcrypt, Goldeneye, Cryptowall, Emotet, jigsaw and Marozka, among many others [17, 18, 19].

In 2020, apart from the pandemic that health and research centers, schools, universities, the government sector and non-profit charities had to deal with, ransomware-type attacks were added. The reason for these cyberattacks was that, by hijacking a critical computer network for these institutions, the probabilities that they will pay the ransom to recover their services are high.

Although initially the ransomware groups promised not to attack these institutions, the ease of obtaining money from information hijacking was and continues to be high. In this context, there were specific cases of “altruistic” actions where cybercriminals donated part of the loot to charities and non-profit organizations, which, of course, does not exempt them from their crime and, therefore, this money was confiscated by the authorities.

Humanitarian reasons do not apply to this type of cyberattack, "if you allow others to access your information, you pay for it", it does not matter if the lives of patients are compromised, there are no scruples, as evidenced in different hospitals

around the world [20, 21], where countries such as the United States [22], Great Britain [23], France, Asia, Europe [24, 25] and the Middle East have been the hardest hit.

Other reasons why the health sector is attacked lie in the fact that its IT infrastructure is weak or with management and administration processes that range from basic to non-existent.

Most clinical devices are networked, such as CT scanners, monitors, radiodiagnostic equipment, etc., which act as weak link points by transmitting data in an insecure way. What is critical about this situation is that millions of patient data are compromised, whose information flows online that can be accessible to those who know how to search them.

In general, disruptive ransomware campaigns are regularly created by cybercriminals, aimed at exploiting weaknesses in certain systems, for example, credentials associated with databases, in particular MySQL and PostgreSQL. The disturbing thing about this situation is that more and more systems are compromised and the worst of the case as [26] points out “as a reminder and warning to those who do not pay for the ransom, more than 250,000 databases of 83,000 MySQL servers and 77 terabytes of leaked data”.

Although the health sector is mentioned as a target for ransomware, it is not the only one, since sectors such as pharmaceuticals, finance, education, transportation and even cybersecurity and technology-based companies are lucrative sources for organized criminal groups.

To carry out a ransomware attack on this type of infrastructure, techniques such as phishing and advanced software such as Ryuk and TrickBot [27, 28] are often used, characterized to collect credentials and filter specific data. Similarly, ransomware has been combined with advanced persistent threat systems (APT) [8] to enhance damage to the interior of a system, either through monitoring the information traffic that circulates through it and stealing confidential data. to sell them to the competition or kidnap them for later payment.

One aspect to reflect on this issue are the attacks on the industry that depend directly on the use of controllers or PLCs for their production processes that, although they present security protocols, are not exempt from being hijacked by these devices with the corresponding consequences, where APTs and now ransomware become the Swiss army knife to carry out targeted attacks with irreparable damage to a logical as well as a physical system.

Attacks of this type are often selective and require time and planning; This is partly due to the fact that a reasonable amount of time is required to know the environment in which the victim moves and then to escalate privileges in the system to capture the greatest amount of information. In the particular case of the IoT, it allows permanent monitoring of what is done within an organization or in the worst case in a city, to have access to its monitoring devices. In this particular case, smart cities in the coming years will increase the technologies related to the IoT, which will not only be aimed at monitoring critical infrastructures, security, transport and health care, but also at the early detection of viral vectors with a view to minimize pandemic risks.

How can you deal with this kind of problem? The answer is to improve the physical and logical protocols and information security, which, of course, is not easy, either because human error is permanently present or because of the progressive advances in cyberattacks, of which no one takes for granted. found out until it's too late. This is where artificial intelligence comes into play, assuming a leading role in automatic decision-making for defense and attack, which will be essential for the coming years. Similarly, if it happens that the system has been compromised, it is advisable not to pay for the demands of cyber attackers. In this way, when the monetary supply is cut, it does not have the objective of hijacking a system, although this is easier said than done, because there are various commercial, corporate, personal, financial and political motives and interests that lead to pay and even shut up and deny that ever there was such an attack and pay for it.

6 Botnet and DDoS

Botnets or zombie networks are defined as a set of computer networks infected by malware, which allows the execution of their inactive processing, in order to increase the computational power to

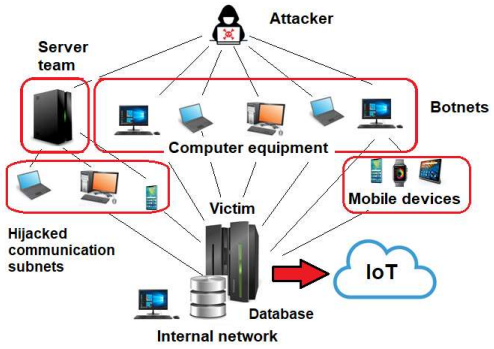

Fig. 1. Representation of a DDoS distributed denial of service attack, where botnets are responsible for spreading malware to other networks and computers by infecting them, then attacking the victim with hundreds of thousands of requests

attack other systems by brute force or through the techniques Denial of Service (DoS) and Distributed Denial of Service DDoS attack. The basic difference between DoS and DDoS lies in the number of infected computers that progressively and repeatedly make requests to a victim system.

This implies that this type of attack demands a set of computer equipment networks infected with malicious software from different sources that facilitate its control, allowing the sending of spam and spreading other types of malwares to continue to progressively infect other networks.

Regarding a DDoS-class attack, [29] points out that: "it consists of a massive attack that seeks to congest the server of a target or consume the entire Internet outgoing bandwidth of the victim's organization." Either of the two attacks makes a network useless, making it collapse for the benefit of the attacker, giving way to infecting and scaling the system, taking over the equipment and information that are available there.

Figure 1 shows in a general way the hierarchical structure of a DDoS and Bonet attack, where the attacker uses a set of previously infected networks, servers and computers, which act as a zombie network or bots in charge of distributing malware to the victim through requests, in order to carry out the DDoS-type attack.

However, this type of attack does not exclude the involvement of any vulnerable mobile technology available, connected to a network such as smartphones, tablets, wearables and of course the IoT.

An inherent characteristic of botnets is that their level of attack is continually technified and diversified, making it almost impossible to eradicate them, an example of this is the InterPlanetary Storm botnet, which detects and evades the security systems of computer networks, whose system operating can be Mac or Android. Another type of botnet is FritzFrog [30] that uses peer to peer (P2) communication to attack SSH servers and Hoaxcalls, facilitating large-scale attacks. This scenario predicts what industry and governments will have to deal with in this decade.

The particularity of botnets is that they are designed and/or rented at the service of the highest bidder to carry out multiple criminal activities that include: DDoS attacks, command execution, sabotage and industrial espionage among others. Any vulnerability that a network system presents will be used by cybercrime for unauthorized access. Examples of the risk that IoT devices expose to Botnet and DDoS attacks are related to the activation of unnecessary or insecure network services that facilitate unauthorized access and control of any service, violating confidentiality, integrity, authentication and/or availability of the information.

There are risks associated with interfaces in charge of managing proprietary or third-party devices, for example, mobile applications, data repositories in the cloud and even the corporate website and the backend APIs (typical of application programming). All these flaws lead to vulnerabilities such as the implementation of weak encryption (or the absence of it) on the data that circulates through the network, as well as the absence of input/output filters.

Other flaws found in IoT devices that can be exploited for unauthorized access are: outdated firmware that lead to the lack of management of encryption processes in transit and validation of updates without appropriate mechanisms for this; use of insecure or outdated software components and libraries; inappropriate use of personal information stored on a device whose degree of security is questionable in addition to the absence of formal permission or informed consent; absence of data encryption and access control.

All these failures converge to the lack of management and administration of IoT devices

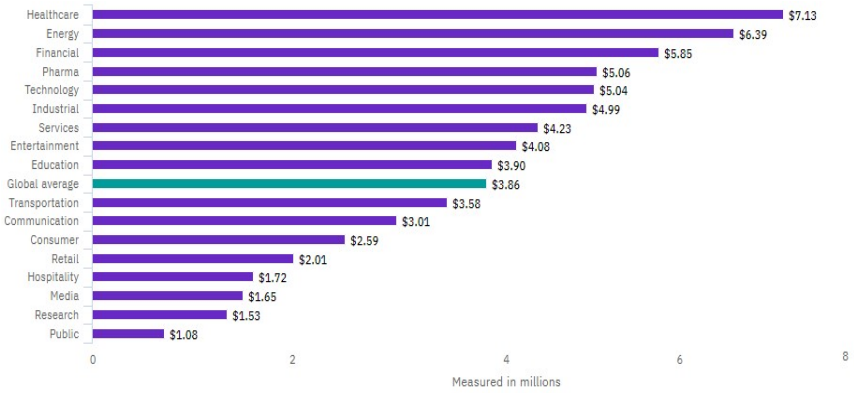

Fig. 2. Average total cost of a data breach by sector [33]

attributed to human errors, which do not comply with the corporate information security standards and/or policies dictated by national and international entities such as the ISO 27000 family of standards. [31, 32].

7 Discussion

The risk of increasing cyberattacks in the coming years is high, this is due to the simple fact that there will be millions of servers around the world that will be compromised due to security failures, where the IoT with its different variants present greater vulnerabilities for the industry and society in general, whose dependence on technology grows day by day. Likewise, the medium-term attack methods are designed to counteract standard security tools and forensic examinations, which entail new advanced malware models that in most could have integrated algorithms based on artificial intelligence (AI).

In this sense, both the way of attack and defense of computer systems must evolve to new levels that will demand significant resources, especially for governments, industry and technology-based companies.

One aspect to take into account is the direct and indirect cost of data breaches, which can take years to correct within an organization. In fact, data leakage and security incidents can lead to the disappearance of an organization, either due to the payment of ransom for the hijacked information, loss of customers and businesses due to bad publicity, system inactivity, detection time and contention of a cyberattack, loss of share value (for those companies that are listed on the stock exchange), demands that this entails due to the exposure of the personal data of thousands or millions of users and non-compliance with the regulations in this regard; that carries regulatory fines that can run into the millions of dollars.

For example, a report by IBM and the Ponemon Institute [33] showed that the average cost of a data breach in 2020 was $ 3.86 million on average. This situation shows that the sector that was hit the hardest was the health sector with a value of more than 7 million dollars, followed by the energy and financial sectors, as can be seen in figure 2.

Based on these facts, it is clear that for the next few years the outlook will not change much, this in part due to the COVID-19 pandemic, which acted as a trigger for cyberattacks to be focused on the health and corporate sectors. However, although the vaccine already exists, preventive isolation and remote work from home will continue for some time to come [34, 35] and, consequently, cyberattacks will be concentrated in these sectors; This suggests that the costs of data breaches may be increased if no action is taken on the matter with regard to cybersecurity.

For example, at the end of 2020, cyberattacks were accentuated in agencies in charge of issuing authorizations for several vaccines against the coronavirus, in particular the European Medicines Agency (EMA). This poses a serious cybersecurity problem for years to come, not just for vaccines being sold on the black market, but for any other essential medicine, where cybercrime has found a near inexhaustible source of profit for profit.

Another aspect to consider are those cyberattacks aimed at stealing the login in the most commercial browsers; this in order to distribute malware aimed at fraud and credential theft. Although current browsers have a high level of security, they are not exempt from advanced cyberattacks that seek to modify DLLs or insert polymorphic malware in cookies and pop-up pages, among others, which are expected to evolve this decade.

Most of the failures mentioned can be solved through corrective actions within a corporate network, such as: firmware update, installing patches issued directly by the provider, encrypting devices with their own passwords and not leaving the factory default one, two-factor authentication (*password + code or 2FA key*), disabling non-essential services of protocols such as IPv6 and IPv4 +, configuration failures in the web interface, configuration of devices to work under internal DNS servers, monitoring of packet traffic in the network for network abnormalities, strong encryption and access controls.

Cyberattacks evolve and therefore, the measures and protection of information must be improved, which is not unnecessary to remember, it is the most important asset of any organization.

There are solutions on the market that minimize the risk of cyberattacks, such as Microsoft's Azure Defender for IoT, which integrates third-party information technology security tools, in such a way that it allows it to work with different devices from recognized IoT providers. Another solution proposed by Amazon Web Services is AWSIoT and AWSIoT Core for public and private networks of low power and wide area LoRaWAN (Low Power Wide Area Network), designed to improve connectivity and security in IoT devices connected to the AWS cloud.

In the case when the crime has been committed and a ransom is requested for the information, it is advisable not to pay and notify the authorities, since, in doing so, what is achieved is to perpetuate the intrusions and maintain these criminal actions that are every more lucrative, due to the fact that it is paid to prevent confidential information from being published, which in many cases, despite being paid, is published on filtering sites combined with the so-called double extortion.

These two modalities are recent; the first is used as additional pressure on the victims to pay, publishing information on those companies or government agencies that have refused to pay, and the second consists of publishing some data on the darknet so that the victim can pay and see that they are talking seriously. In this regard, there are nations that prohibit the payment of these ransoms under penalty of heavy sanctions. Employee training and awareness is a critical part of a company, since it is enough for a single employee to violate safety standards and / or policies to compromise the entire system. Now, in the event that the cyberattack has been completed, it is advisable to establish contingency plans for technical incidents and commercial recovery, which are supposed to have been previously designed to deal with this type of scenario.

Based on the above, various government agencies and the technology industry are looking for plausible solutions that make it possible to nullify or at least minimize the negative impact of cyberattacks and cyber espionage on IoT systems.

For example, the ETSI (*European Telecommunications Standards Institute*) is a European body that launched the security standard ETSI TS 103 645 [36]; which includes data protection and security in household appliances and consumer devices such as smart cameras, access controls, wearables and consumer systems that include IoT gateways, base stations and hubs, portable devices, home automation systems, connected gateways, door lock and window sensors.

The objective of this standard and others under construction are aimed at unifying criteria that facilitate both organizations and nations to keep a strict control of the IoT devices that come out and circulate in the market. Although common agreements need to be defined at the global level that allow defining and assigning responsibilities and ownership in matters of security and data management, it is a matter of time before they reach an agreement, this in part due to the boom in the development and implementation of new technologies. IoT for the next few years.

On attacks focused on the capture of information stored in the cloud, it is the holy grail of cybercrime, because they would have control of all the information of an organization and, therefore,

all its assets would be compromised, with a devastating impact on the services provided, ranging from the extortionate payment of large sums for releasing the information, to the periodic payment of sensitive information from both the company and its clients, even using various subterfuges to apply them to the latter.

However, despite concerns at the security level, for the present decade the increase in networks composed of intelligent IoT devices and variants thereof will be even greater, involving various emerging technologies to expand their services, such as those where not only they manage data packages, but rather energy packages through the different nodes of the network, who will be in charge of calculating the most optimal route to their destination. This new economic environment opens up new business opportunities for the services industry, energy distribution and smart monitoring of cities, homes and people, and unfortunately new opportunities for cybercriminals and political destabilizing cyber groups, not to take action on the matter for part of the competent authorities.

7 Conclusions

Information security for the next few years will be increasingly compromised by continuous advances in computer systems and advanced algorithms. This has serious implications on the risk of compromising sensitive data to criminal organizations or states interested in profiting from the vulnerabilities of others, or destabilizing the economy of their counterparts. The truth of all this is that companies must be better prepared to deal with this type of scenario. The rule is simple, a company that does not invest in cybersecurity is doomed to disappear. It goes without saying that the regulations and fines for breach of data protection are leading the industry and service companies to take this issue seriously, because there is not only the pecuniary punishment, but also the reputation and potential lawsuits to which it is expose for not complying with the law in this regard.

In the case of IoT, things are not going well, because the above applies equally to companies that trade and use IoT devices.

It is advisable to take into account the use of encryption in an expansive way, AES-XTS [37] block encryption for Flash drives and secure boot based on the RSA algorithm and/or variants, automate security thereby minimizing human risk, establish business continuity plans and decoy teams, permanently train employees, perform online and offline data backups, use of blockchain as a system to monitor transaction and data processing, among other aspects with a view to minimizing risk.

It is undeniable that the security factor is fundamental and its relevance in any communication system cannot be overlooked, which will demand new developments in hardware as well as in software; so much so that the collection of personal data by IoT devices will increase in the coming years, forcing the adoption of new encryption techniques such as homomorphic cryptography [38] and protocols that involve confidential computing with security level 4 [39], guaranteeing the user that their data is safe.Also, the incorporation of applications related to artificial intelligence (IAoT) is contemplated, ranging from predictive learning, through interactive audio and voice systems to monitoring and in situ human-device interaction, for example, autonomous vehicles, civil drones and military, clinical monitoring, logistics and traceability among others

For this decade, the modalities of malware and cyberattacks will continue to evolve, so it is necessary to prepare for it. Ransomware campaigns will become increasingly aggressive, with higher ransom demands, although the attacks are concentrated in organizations, it does not imply that an ordinary citizen is exempt from it, it all depends on the degree of interest of the cybercriminals or who I hired them. Coordinated attacks can be more effective and lucrative, therefore, it is advisable not to lower your guard and be vigilant, not only the personnel in charge of the systems and networks, but also of each employee, since not only corporate information is being compromised but the information of the staff and even their families.

It is important to anticipate what is coming for this decade in terms of emerging technologies such as 5G networks (including 6G), whose implementation has begun and has also begun to

show weaknesses in terms of security, such as user location and theft of data, opening countless opportunities to hijack, scale a system and steal information on a massive scale through attacks on certain protocols and DDoS and APT attacks. It is worth mentioning in this regard that, with services focused on the mobile consumer, security, trust, convenience and ubiquity are factors to consider under current standards and future communication technologies.

To conclude, with the current geopolitical dynamics that in the future show that the tensions between the great superpowers will increase even more, the ransomware, APT and DDoS attacks will be focused on attacking critical infrastructures and industry of a nation.

In this sense, the industrial sector and governments must anticipate this type of attacks, requiring seeing data security as an investment that demands ideal technical and technological resources, as well as designing and implementing incident response plans, enforcing regulations in cybersecurity among many other aspects.

References

1. **Márquez, D. J. (2019).** Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas. Revista de Bioética y Derecho No. 46, pp. 85–100. DOI:10.1344/rbd2019.0.27068.
2. **Lin, J., Chen, W., Lin, Y., Cohn, J., Gan, C., Han, S. (2020).** MCUNet: Tiny deep learning on IoT devices. Advances in Neural Information Processing Systems 33 NeurIPS´20, DOI: 10.48550/arXiv.2007. 10319.
3. **Harth, N., Anagnostopoulos, C., Pezaros, D. (2018).** Predictive intelligence to the edge: Impact on edge analytics. Evolving Systems Vol. 9, pp. 95–118. DOI: 10.1007/s12530-017-9190-z.
4. **Mekki, K., Bajic, E., Chaxel, F., Meyer, F. (2018).** A comparative study of LPWAN technologies for large-scale IoT deployment. ICT Express. DOI: 10.1016/j.icte.2017.12.005.
5. **Ackerman, D. (2020).** System brings deep learning to “internet of things” devices. MIT News on campus and around the Word. https://news.mit.edu/2020/iot-deep-learning-1113
6. **Acharya, S., Tiwari, N. (2016).** Survey of DDoS attacks based on TCP/IP protocol vulnerabilities. IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 18, No. 3, pp. 68-76. DOI: 10.9790/0661-1803046876.
7. **Sistu, S., Liu, Q., Ozcelebi, T., Dijk, E., Zotti, T. (2019).** Performance evaluation of thread protocol based wireless mesh networks for lighting systems. International Symposium on Networks, Computers and Communications (ISNCC), Istanbul, Turkey, pp. 1–8. DOI: 10.1109/ISNCC.2019.8909109.
8. **Márquez, D. J. E. (2017).** Armas cibernéticas. inteligencia artificial para el desarrollo de virus informáticos letales**.** Revista Ing.USBMed, Vol. 8, No. 2, pp. 48-57. DOI: 10.21500/20275846. 2955
9. **CSIS (2021).** https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
10. **Luoung, H. T., Phan, H. D., Chu, D. V., Nguyen, V. Q., Le, K. T., Hoang, T. L. (2019).** Understanding Cybercrimes in Vietnam: from leading-point provisions to legislative system and law enforcement. International Journal of Cyber Criminology, Vol. 13, No. 2, pp. 290–308. DOI: 10.5281/zenodo.3700724.
11. **Baezner, M. (2018).** Hotspot analysis: use of cybertools in regional tensions in Southeast Asia. Zurich: Center for Security Studies (CSS). Cyber operations in the gray zone, 27.
12. **Bullee, J. W., Montoya, L., Junger, M., Hartel, P. (2017).** Spear phishing in organisations explained. Information and Computer Security, Vol. 25, No. 5, pp. 593–613. DOI: 10.1108/ICS-03-2017-0009.
13. **Ortiz, C. N. J. (2019).** Normativa Legal sobre Delitos Informáticos en Ecuador. Revista Científica Hallazgos21, Vol. 4, No. 1, pp. 100–111.
14. **Márquez, D. J. E. (2020).** Internet of things and distributed denial of service as risk factors in information security. Chapter 19 Bioethics in Medicine and Society, DOI: 10.5772/ intechopen.94516.

15. **Associated Press. (2021).** Suspected Russian hack fuels New US action on cybersecurity. https://www.voanews.com/usa/suspected-russian-hack-fuels-new-us-action-cybersecurity
16. **Sanger, D. E., Perlroth, N. (2020).** U.S. to accuse China of trying to hack vaccine data, as virus redirects cyberattacks. https://www.nytimes.com/2020/05/10/us/politics/coronavirus-china-cyber-hacking.html.
17. **Connolly, Y. L., Wall, D. S. (2019).** The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. Computers & Security, No. 87, 101568. DOI: 10.1016/j.cose.2019.101568.
18. **Maurya, A. K., Kumar, N., Agrawal, A., Khan, R. A. (2018).** Ransomware: Evolution, Target and Safety Measures. International Journal of Computer Sciences and Engineering, Vol. 6, No. 1, pp. 80–85. DOI: 10.26438/ijcse/v6i1.8085.
19. **Brewer, R. (2016).** Ransomware attacks: detection, prevention and cure. Network Security, Vol. 2016, No. 9, pp. 5–9. DOI: 10.1016/s1353-4858(16)30086-1.
20. **Harkins, M., Freed, A. (2018).** The Ransomware Assault on the Healthcare Sector. Journal of Law & Cyber Warfare, Vol. 6, No. 2, pp. 148-164.
21. **Collier, R. (2017).** NHS ransomware attack spreads worldwide. CMAJ: Canadian Medical Association journal (journal de l'Association medicale canadienne), Vol. 189, No. 22, E786–E787. DOI:10.1503/cmaj.1095434.
22. **Branch, L.E., Eller, W.S., Bias, T.K., McCawley, M.A., Myers, D.J., Gerber, B.J., Bassler, J.R., (2019).** Trends in Malware Attacks against United States Healthcare Organizations, 2016-2017. Global Biosecurity, Vol. 1, No. 1, pp. 15–27. DOI: 10.31646/gbio.7.
23. **Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Flahault, A. (2020).** Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, Vol. 20, No. 1. DOI: 10.1186/s12911-020-01161-7.
24. **Yeo, J., Vander Ende, R. (2017).** Cyber evolution. En Route to Strengthening Resilience in Asia-Pacific. FireEye.
25. **European Commission. (2020).** Cybersecurity. Our digital anchor a European perspective. Publications Office of the European Union.
26. **Johnson, D. B. (2020).** New ransomware campaign exploits weak MySQL credentials to lock thousands of databases.
27. **Unterfingher, V. (2020).** Ryuk ransomware – untangling a convoluted malware narrative.
28. **Gittins, Z., Soltys, M. (2020).** Malware persistence mechanisms. 24th international conference on knowledge-based and intelligent information & engineering systems. Procedia Computer Science Vol. 176, pp. 88–97. DOI: 10.1016/j.procs.2020.08.010.
29. **Astudillo, B. K. (2019).** Hacking ético. Tercera edición, Ed. Ra-ma.
30. **Anonymous news (2020).** Massive new botnet discovered. Computer Fraud & Security, Vol. 2020, No. 9, p. 3. DOI: 10.1016/S1361-3723(20)30092-0.
31. **Baena, G. R., Mendoza, M. R., Joel, C. E. (2019).** Importancia de la norma ISO/EIC 27000 en la implementación de un sistema de gestión de la seguridad de la información. Revista contribuciones a la Economía, pp. 1– 13.
32. **MinTIC (2016).** Guía para la Implementación de Seguridad de la Información en una MIPYME (Norma No. 1.2).
33. **IBM Security (2020).** Informe sobre el coste de una brecha de datos. Madrid, España, IBM, España, SA.
34. **International Labour Organization (2020).** An employers' guide on working from home in response to the outbreak of COVID-19. Geneva: International Labour Office. www.ilo.org/publns
35. **Clifford, S., Quilty, B. J., Russell, T. W., Liu, Y Desmond-Chan, Y. W., Pearson, C. A. B., Eggo, R. M., Endo, A., Flasche, S., Edmunds, W. J. (2020).** Estrategias para reducir el riesgo de reintroducción del SARS-

CoV-2 de viajeros internacionales. MedRxiv´20. DOI: 10.1101/2020.07.24.20161281.

36. **ETSI (2020).** CYBER; cyber security for consumer internet of things: baseline requirements. ETSI EN 303 645 V2.1.1. European Standard.
37. **Luo, C., Fei, Y., Ding, A., Closas, P. (2019).** Comprehensive side-channel power analysis of XTS-AES. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 38, No. 12, pp. 2191–2200. DOI: 10.1109/TCAD.2018.2878171.
38. **Zhao, E, M., Geng, Y. (2019).** Homomorphic encryption technology for cloud computing. Procedia Computer Science, Vol. 154, pp. 73–83. DOI: 10.1016/j.procs.2019.06.012.
39. **FIPS 140-3 (2019).** Federal information processing standards publication (Supersedes FIPS PUB 140-2). Security requirements for cryptographic modules. Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8900. DOI: 10.6028/NIST.FIPS.140-3.
40. **Turjman, F. A. (ed.) (2019).** Artificial intelligence in IoT. Transactions on Computational Science and Computational Intelligence. Springer.

Article received on 01/04/2021; accepted on 23/07/2022.
Corresponding author is Jairo Eduardo Márquez Díaz.