We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

5,300
Open access books available

130,000
International authors and editors

155M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS BOOK CITATION INDEX INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

Chapter

Internet of Things and Distributed Denial of Service as Risk Factors in Information Security

Jairo Eduardo Márquez Díaz

Abstract

Society is increasingly dependent on technology and an example of this is the constant monitoring of large cities, which has become common and the future trend is for it to increase based on what happened with the COVID-19 pandemic. This monitoring brings with it a series of problems at the information security level at different levels or levels. Based on this fact, it addresses how the Internet of Things (IoT) can be subject to potential distributed denial of service (DDoS) attacks and the danger it poses to society. In this sense, other types of vulnerabilities are exposed, such as crypto hacking, advanced persistent threats (APT) and ransomware, which use artificial intelligence to improve their attack techniques. This poses a potential risk to society from cybersecurity regarding the use and manipulation of information, either by governments, the military and organized criminal groups, de facto violating human rights.

Keywords: advanced persistent threats, artificial intelligence, big data, cybersecurity, cloud computing, DDoS, internet of things

1. Introduction

Disruptive technologies such as artificial intelligence (AI) have been rapidly being incorporated into different scientific fields and industry, becoming a support for technologies such as: big data, data science, the internet of things (IoT), computational linguistics, intelligent computing, assisted technologies, advanced robotics, among others. Also, AI has been incorporated in fields such as medicine, an example of this are systems for the early detection of COVID-19 through the use of techniques such as deep learning and machine Learning [1, 2] for the analysis of cellular and protein images, as well as the study of molecular and cellular dynamics among other aspects.

Other fields in which AI can be found are: manufacturing and logistics, industrial processes of various kinds, finance, adaptive education, diagnostic systems, micro and nanoelectronics, precision agriculture, transport, telecommunications, defense system, etc. even in the video game and toy industry.

A peculiarity of AI is that with the current computational potential it can be applied practically in whatever is desired. For example, in the development of advanced robotic systems, both software (chatbots) [3] and hardware, which allow emulating certain traits and interaction with the human being. Similarly, AI is

incorporated into information and communication technologies, in the control and monitoring devices of homes, buildings and cities (Smart Cities), which converge to the so-called Internet of Things (IoT), which involve sensory, cloud computing, data science and cybersecurity among other disciplines.

In terms of security, standard and AI-mediated IoT present a debatable level of security. This is due to the fact that the base code of the firmware or operating system of these devices [4], does not have an acceptable level of security and, as they are permanently connected to a communication network, their exposure to computer attacks is high. This type of failure is attributed in part to device design and manufacturing failures, where the safety factor was underestimated, without taking into account that the devices and sensors under the IoT scheme are supported under Internet protocols and standards, and although they do not use them in their entirety, it does not imply that they are exonerated from being exploited by some type of malware.

In this sense, hacking this type of system allows us to steal data not only from homes, but from hospitals and research centers, industries, vehicles, weapons and drones, even causing accidents or taking lives selectively. In the case of robots and cobots, cameras, toys (including sex toys), printers and household appliances, among other devices connected to the internet or through a mobile device, can be maliciously intervened if they are not configured correctly regarding their access. Cyberattacks on these devices are often attributed to botnets; since they allow attacks by distribution of denial of service (DDoS), oversaturating Internet access traffic in order to disable or take control of the network to which the devices are connected. When this is achieved, access to the privacy of the victim or target is taken for granted without their being aware of it until it is too late.

Under this type of attack, what is sought is to collect information from the victim that allows obtaining bank access codes, personal and/or corporate email codes in order to continue climbing to steal sensitive information, images or intimate videos that lead to extortion, among others. For example, in 2016 an attack on Europe and North America was used under the DDoS modality [5], using the IoT [6] to disable the DynDNS systems (Dynamic Network Services, Inc.), operated by domain name providers (DNS), this caused the denial of access to internet platforms and services. Also, this type of attack seeks to steal sensitive corporate information to be sold to the competition, destroy it if necessary when there is a contract involved, extort money from the target or destroy critical facilities for terrorist or military purposes.

The problem with botnets is that they will continue to grow as the number of vulnerabilities increases in devices connected to the Internet in the coming years, in addition to other types of vulnerabilities to which a communication network of any industry or public service is exposed or private. This statement is based on the fact that the number of IoT devices connected with other disruptive technologies are growing exponentially, where household appliances and all types of electronic devices are being permanently managed and administered via wired or wireless, making them much more vulnerable to various types of cyberattack.

2. Internet of things (IoT)

The internet of things is defined as the set of electronic devices connected to the internet, whose function is aimed at collecting various information that can be directed to the control of actuators that activate other systems (lights, blinds, thermostat, air conditioning, etc.). Also, it allows the collection of data based on the monitoring or census of physical–chemical or biological variables, communication

between devices and human-devices, identification, location and monitoring, among others. The IoT is in various scenarios; from the home (Smart home), through industry and services, to the health sector (eHealth), transport systems (navigability and predictive maintenance) and infrastructures of a city (bridges, viaducts, buildings, etc.) that converge to the concept of Smart Cities (Smart energy and Smart retail). Likewise, the sensors can be controlled and/or monitored from a central or mobile device, there are even other more advanced approaches focused on the energy industry, in order to optimize communication processes and broadband efficiency, known as Internet of Things-Grid (IoT-G) [7].

A notable characteristic of the IoT is that it has diversified to such an order that there are billions of devices permanently connected to the web, and with the rise of 5G technology, even greater growth is expected in the coming years, which He envisions drastic changes in Industry 4.0, where AI is going to play a key role in this context. Under this dynamic, researchers, scientists and engineers face emerging challenges in designing IoT-based systems that can be efficiently integrated with 5G wireless communications [8]. This technology is immersed in society, which in many cases goes unnoticed. The truth is that the volume of information that is permanently recorded is colossal, where technologies such as data science, big data, advanced analytics and Artificial Intelligence, among other disciplines, contribute their own for the treatment of this information.

It is worth mentioning that in technical terms the IoT works under the TCP/IP model, in which various protocols related to data transfer operate. For example, the Internet Protocol (IP) is the one that allows interoperability between devices, where the IPv4 version is definitively replaced by IPv6 in 2020, in which the organization of the IP addresses of computers and devices is expanded and improved in various types of communication networks.

There are protocols dedicated to the IoT apart from HTTP (Hypertext Transfer Protocol) such as: OCF (Open Connectivity Foundation), MFi (Made For iPhone/iPod/iPad), AllJoyn, DDS (Data Distribution Service), Thread, HomePlug and HomeGrid, AMQP (Advanced Message Queuing Protocol), CoAP (Constrained Application Protocol), MQTT (Message Queuing Telemetry Transport), XMPP (Extensible Messaging and Presence Protocol) and OPC UA (Unified Architecture), considered as a new generation standard. The operability of these protocols is based on the TCP or UDP protocols. In the case of the UDP protocol, it presents certain limitations in terms of connectivity and functionality, specific to its architecture.

Regarding the TCP/IP model, it exhibits vulnerabilities in each of its layers (Application, Transport, Internet and Network) that can be exploited [9]. For example, at the network layer, common problems are confidentiality and access control, which can be compromised through network hardware, that is, through IoT devices. At the network layer, the attacks are carried out at the level of modifying or canceling a datagram associated with the IP of a device, using techniques such as sniffing and spoofing in the ARP protocol or disabling the MAC filter, among others.

At the network infrastructure level, the transport layer fulfills the function of transmitting data via TCP or UDP protocols over IP datagrams. At this point, security problems are presented at the level of authentication, integrity and confidentiality of the information. Consequently, denial of service attacks can be performed by obstructing the flow of data by disabling communication between client and server. Other attacks that may occur are: pseudo-random subdomain attack (PRSD), IP Flooding, distributed attack, snork, ping of death, smurf, Spoofing for SYN flood DoS attacks TCP/SYN, flooding and teardrop, NTP amplification, attacks ICMP (ping), UDP Flood, HTTP Flood, SSL (Secure Sockets Layer)/TLS (Transport Layer Security) renegotiation, among others, where each one takes

advantage of the design vulnerabilities of the layer itself. In the case of the internet layer, the attacks are conceived at the level of the fragmentation of IP datagrams, masking them by others that compromise the data that circulates through different points of a network.

As can be seen, the TCP/IP model since its creation has inherent weaknesses in its own design that can be exploited to carry out various types of attacks [10, 11]. In the particular case of IoT devices, they become perfect targets for cybercrime and industrial, military and government espionage, which, as can be seen, the attack vectors come from various sources, which are not necessarily organized crime.

There are other security factors to take into account about the IoT, which is related to the use of different technologies such as Wireless Sensor Networks (WSN), Near Field Communication (NFC) and Radio Frequency Identification (RFID) that are implemented in standard mobile devices, where each of them presents its own vulnerabilities [12]. Each technology requires specific protocols [13], to which is added 5G technology, whose emerging applications open up a myriad of applications, such as new attacks on advanced networks, for example, HealthTech and BioTech-type applications.

Regarding the standard communication protocols such as Ethernet, Wi-Fi and Bluetooth, others related to the application layer are presented specifically designed for a company's own products, so they are not considered as standardized, for example: Nest, MFI, Open Interconnect Consortium (OIC) and The AllSeen Alliance. Under this scenario, each industry that works with IoT develops its own protocols without universal unification, which guarantees connectivity compatible with devices from other manufacturers; This creates a security breach that can be exploited by cybercrime. An example in this regard was an attack that occurred in 2020 in the United States, using the Drovorub malware [14], the objective of which was to massively hack IoT devices in order to access wider communication networks.

3. Distributed denial of service and IoT

The Internet of Things is found in various devices as indicated by [13], in household appliances, smartphones, smart clothes, wearables (bracelets, virtual reality glasses, etc.), smart TVs, game consoles, transportation systems, buildings (security cameras, air conditioning, access controls, etc.), public infrastructures (bridges, highways, parks, etc.), public services, industrial components (e.g. SCADA systems) [15], systems transportation, etc.

A particularity of the IoT as mentioned above, is the connection between devices and the exchange of information between them under the TCP/IP model and their own custom-designed protocols. This poses great challenges in terms of information security, which as [16] state, there are attacks on devices connected to the Internet, in which there is fear of surveillance and concern for privacy. The reason for this, underlies as [17] points out, is that the IoT is presented as a source of data collection that grows exponentially and, consequently, every object becomes a source of information.

A critical point of the IoT in terms of information security is distributed denial of service (DDoS) attacks, whose objective is focused on disabling the continuity of communication of devices connected to a network, affecting the switched flow tables, data on a network, bandwidth and latency, taking advantage of the weaknesses of the OSI (Open System Interconnection) model (see **Figure 1**), in which attacks can be carried out at the transport, network and application layers, as well as DNS, SMURF and ACK amplification type attacks, among others.

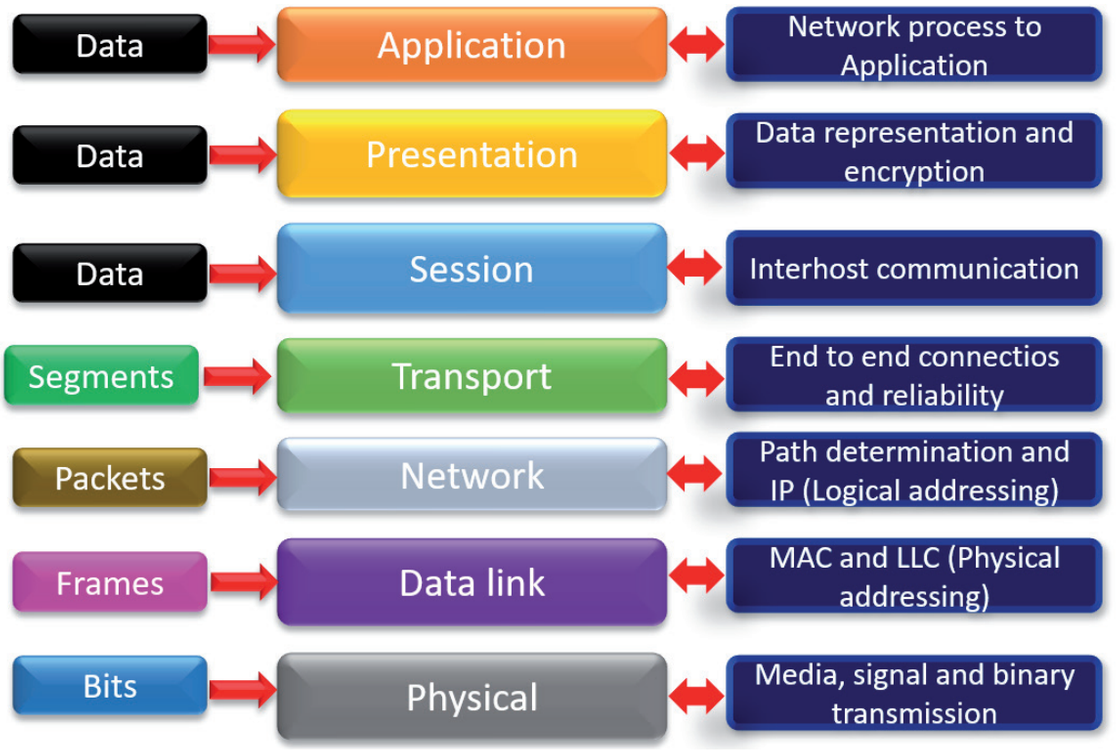

Figure 1.
Layers or levels of the OSI model, elements that it manages and functions.

Some effects of these attacks consist of making multiple requests to one or more servers (web, proxy, email, database, etc.), with the aim of saturating the network until it collapses. Also, brute force attacks can be carried out through specialized malware that is in charge of scanning the target network in search of IoT devices in order to obtain passwords, hijack them and link them to a botnet [18], which is basically a malware that takes advantage of browser vulnerabilities by installing itself on computers and/or servers.

The main characteristic of a botnet is that it infects the greatest number of systems forming the so-called "zombie" networks; which are controlled by Command & control type servers, which increase the capacity for DDoS and Spam attacks, among others, to specific objectives, which are normally companies and/or corporations, critical infrastructures such as transport, essential public services, health sector, food, etc., although attacks directed at a particular individual are not ruled out.

Regarding the defense mechanisms available to counter a DDoS attack, these present certain limitations such as the lack of resources at the software or hardware level in a network, or due to the technical and technological flexibility that a network has to deal with this. Type of attack. In this sense, the manifestation of potential risks attributed to technologies such as IoT with respect to DDoS, are expressed through security flaws that grow day by day, not only due to the number of devices, but also due to their diversification of these in multiple fields of industry, transportation, health and entertainment among others, becoming a global security problem.

The motivations for carrying out this type of attack are diverse and varied, ranging from personal or corporate resentments, through espionage, blackmail and extortion, to unfair competition or political and military ideologies. The growing reason for these attacks lies in the various vulnerabilities that can be exploited in IoT devices, whose manufacture questionable puts their security among them, as well as the poor configuration of the devices or portals by the personnel in charge.

Another aspect to be mentioned as a reference to the vulnerability of the IoT is related to the pandemic caused by COVID-19, whose attacks in the first half of 2020 increased alarmingly worldwide [19], in particular on websites of medical organizations, educational and administrative platforms, online gaming platforms and delivery services of various kinds. With this type of attack, it was shown that cybercriminals were not very interested in the social and humanitarian factor.

It is worth mentioning that DDoS attacks require poorly configured computer networks and servers, which once hijacked are connected to a Zombie network (**Figure 2**). This strategy applied to IoT devices acts as a connection bridge to be used as digital weapons of attack and espionage, expanding the coverage of the zombie network, boosting thousands or millions of times the level of request to the servers targeted by the attack. The problem with an attack on this scale is that the IoT is in continuous growth, that as [20] affirms only by 2020 there will be more than 50 billion connected devices (omnipresent) in cities, that is more than the estimated world population for this date (7.5 billion). Now, with the problem of the pandemic, there are hundreds of projects that promote the IoT for the permanent monitoring of cities, homes, hospitals and transportation systems among other critical systems of cities in the coming years, all aimed at minimizing future pandemics, for causing the number of devices to skyrocket to significantly larger numbers.

Another issue to take into account is related to metropolitan security, in which technologies such as cameras, sensors and drones are increasingly being incorporated, connected via IoT devices and mobile telephony. In the worst case scenario, when hacking this type of infrastructure, a city would be at the mercy of an attacker having access to infinite data. Now, this type of attack would not only be orchestrated by organized crime and terrorists, but by the governments themselves and the military, as noted above, with the exclusive purpose of monitoring each

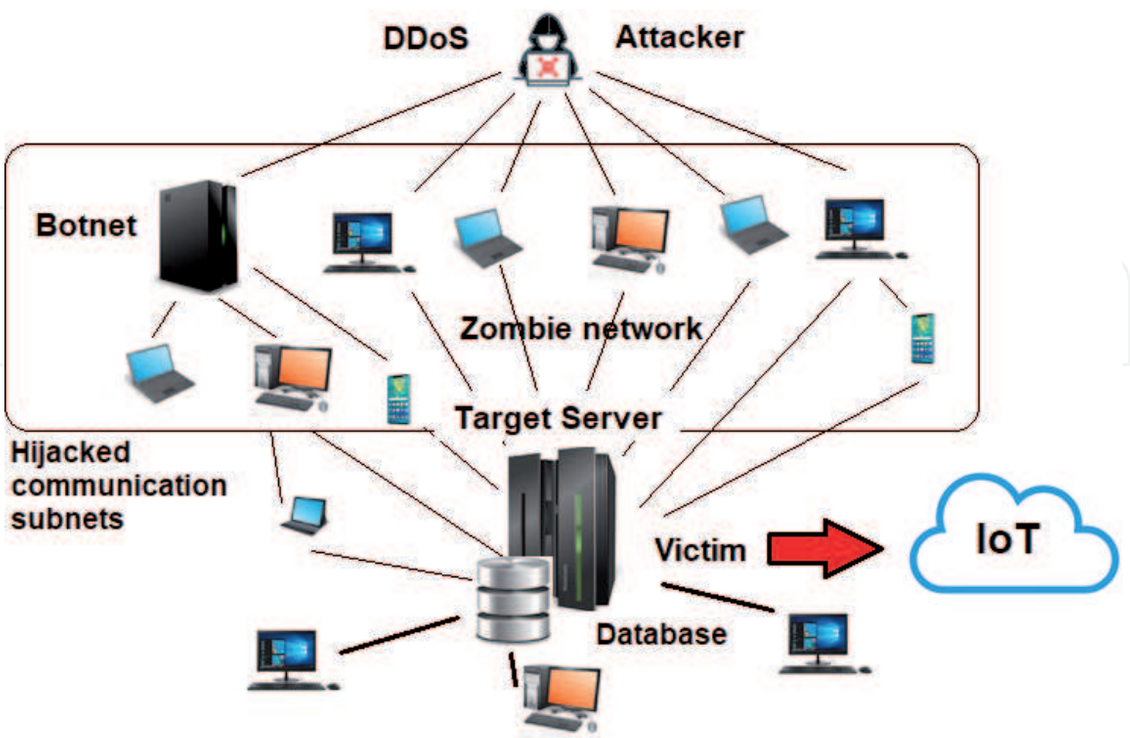

Figure 2.
Graphical representation of a distributed denial of service (DDoS) attack on an IoT system. As can be seen, a set of botnet is used to attack the victim, which in this case is a server that manages information from devices related to the IoT. The result of this attack is to have access to the database hosted on the server, to the control of the network connected to it and to the IoT devices.

individual and society permanently and with impunity, violating human rights. For example, China under his regime [21], is one of the countries that has the most information on its population using various technologies such as biometric registration and facial recognition systems, integrated with databases (includes DNA databases) managed and administered through artificial intelligence. Another example is the National Security Agency (NSA) and the CIA of the United States, which repeatedly violate human rights spying not only on their own community but on the entire world [22], as well as other agencies from other countries [23].

Returning to the topic of DDoS, there are various mitigation techniques for an attack of this type, whose large-scale feasibility is debatable. This is due in part to the efficiency and complexity of being able to implement these techniques. For example, a recent proposal is based on the use of blockchain technologies and Smart Contracts [24, 25] that have the necessary infrastructure to preserve the design and stability in terms of the development of a protocol that supports DDoS-type attacks. The proposal takes as support cloud computing, whose degree of security is high, due to the way data packets are filtered, where the system consists of a set of devices or programs (Firewalls and Proxy) configured in such a way that limits the passage or access of information in a network under certain rules and protocols.

4. Security factors in IoT

In terms of security, the IoT presents various weaknesses depending on the type of technology and application it is given, where DDoS takes advantage of, as do other variants such as low-speed DDoS (LDDoS) [26], which hides its traffic equivalent to normal traffic. Its origin is based on LDoS attack methods, which include variants such as reduction of quality (RoQ) and application servers (LoRDAS attacks). Another type of weakness attributed to the protection of information is focused on the service provider (DPS), which apart from implying additional costs, can lead to a decrease in the performance of the service and security problems, so you must be careful with whom you contract x and y services.

There are security proposals for the IoT, such as: collaborative defense using VNF (Virtual Network Functions), the use of DOTS protocols (DDoS Open Threat Signaling) [27], the exchange of events based on FLow (FLEX) and obfuscation techniques [28], among others. Although they are very good proposals, the problem is still open in establishing ideal protocols that allow confronting large-scale DDoS attacks, in which a greater degree of sophistication, duration and frequency is increasingly observed. In this sense, the use of Artificial Intelligence (AI) initially allows detection using techniques such as advanced neural networks [29] and machine learning [30], among others [31, 32].

One aspect that relates the IoT to AI and cybersecurity, are the failures at the hardware level. For example, design errors in Intel, AMD and ARM processors detected in the kernels, which were exploited by the Meltdown and Specter malware [33]. These errors allowed these malwares to access key parts of the processors by stealing security keys [34]. These failures have opened controversy, whether they were really design problems or were left on purpose for industrial or government espionage, hence policies have been implemented where countries such as the United States, China and Russia, among others, develop their own processor technology to minimize the risk of spying or hijacking in the event of a cyberattack. The implications of this type of attack show the fragility that exists in technology, where the common user has no idea what may be happening with their personal information stored on any electronic device. Seen in this way, society's ever-increasing dependence on technology poses new challenges in terms of security, which must

be carefully reviewed, since one would be at the mercy of government cybercrime without even knowing it.

In the case of IoT, it is that as the collection and analysis of information from various devices increases, not only the industrial and services sector (Industry 4.0) is compromised, but the entire technological infrastructure on which society is based, increasing the security risks, where data grows at ever increasing rates exceeding the Exabyte order. Just imagine the unauthorized access by organized crime or governments to predictive systems, not only in the industrial field, but also in the military, financial, health and critical infrastructures, among others, kidnapping and/or modifying information with impunity, the damage would be practically irreparable adding to a high cost of lives.

5. Implications of the IoT in the healthcare sector

The IoT is increasingly being incorporated into the health sector from different fronts, even under other disruptive disciplines such as E-health (or e-health) composed of technologies such as: electronic medical record, E-learning, B-Learning, telehealth that includes telemedicine, Mobile-Health, among others. Also, the Wearables are found along this same line; considered as electronic devices for permanent monitoring of vital signs, detection of arrhythmias, measurement of glucose levels and biometric marker systems, among other functions. These devices are usually found in a person through accessories such as: watches, bracelets, glasses, rings, underwear and outerwear, among other elements, so in this context the IoT changes to the term Internet of Wearables Things (IoWT) [35, 36]. In the case of disease monitoring through the biosignal registry, the term Internet of Medical Things (IoMT) has been coined [37], which uses devices with RFID (Radio Frequency identification) and NFC (Near Field Communication), being useful for monitoring biosignals in clinical and epidemiology trials and research, facilitating obtaining real-time data and conducting traceability studies and identification of variables, communication between devices and patient location; this makes it easier for medical personnel to offer personalized attention and follow-up on a certain treatment.

It goes without saying that spending on IoT solutions for health care will exceed one trillion dollars in the coming years, this in part because of COVID-19 and other variables such as the increase in the number of people who pass into the elderly and the increase in chronic diseases that demand special care, where technology contributes its own in this regard.

All these technologies collect a large amount of medical data permanently from human activities, which as [38] points out, with the use of IoT allows access to massive data on population health and although its individual use is of enormous benefit for clinical medicine, on a large scale it represents a revolution for global health. This leads us to think about the responsibility that falls on those who have access to this information and the risk that it falls into the wrong hands. Therefore, the concern about the security of this data is justified, since its interception and manipulation imply a risk and violation of the patient's privacy rights, added to the irreparable damage that this entails to their family and health institutions, so it requires a detailed study on these aspects, as stated [39–42].

The truth of all this is that the volume of data grows continuously, demanding new technologies for both storage and processing, such as data science, big data, artificial intelligence and cloud computing among others, all of them managed through communication networks. In terms of security, the institutions establish policies aimed at minimizing the risk and vulnerabilities of these systems.

However, the probability of a computer attack is latent, and as has been pointed out, it can come from various sources, which are not only external but internal. For example, active or inactive dissatisfied personnel who provide information about the infrastructure of the hospital's communication systems to third parties, bribes and corporate infiltration, among other factors, make guaranteeing the security of clinical information a real challenge not only for the personnel in charge, but for each person who works in the institution. It goes without saying that it only requires a device failure to facilitate unauthorized access to a network and, therefore, to the information that circulates through it.

Well managed IoT and its variants like IoWT and IoMT reduce security flaws, but they are not eliminated. Seeing this problem on a large scale, a country's health system can be compromised, let us remember that in 2020 there were attempts to hack hospitals and research centers that were working on the vaccine and control of COVID-19. Therefore, no institution is safe from a cyberattack and even less if they have profit, political or terrorist purposes. Let us just imagine the scenario of a politician, activist or social leader, who is hacked into clinical information by intervening, deliberately and selectively altering procedures and/or medication in order to threaten his life. Although it sounds cinematic, the possibility is real, in the same way, various IoT devices can be intervened to monitor and intercept information.

In reality, without going into conspiratorial arguments, there are no limits to what can be done when you have free access to sensitive information from an organization, particularly clinical data. The task of exploiting the vulnerabilities of an IoT system is not easy, but neither is it impossible, since there are various techniques, software resources and online services such as the Deep Web and Darknet that allow this task to be carried out systematically in a relatively short time. In the government field, their agencies have unlimited resources to carry out DDoS attacks, so they are more difficult to detect and track, so they are literally ghosting that move on the network, even from the deep web itself.

6. Cloud computing and big data

Cloud computing is understood as a model of information technology service on demand, which makes available to users a vast network of servers on which various types of applications run, storage and processing of large volumes of information and internet services on demand, business solutions, among others. For this, it uses three models of Cloud services: IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service), where each one differs in terms of storage capacity, services and security, among others.

Due to its scalable characteristics of cloud computing, the management of information for the management of IoT technologies and related projects such as big data, advanced analytics and artificial intelligence, among others, is unlimited, so large and small companies hire this type of service, since they do not require their own technological infrastructure minimizing costs, just as the information is available at any time and place. As an additional fact, there are currently three major cloud computing service providers: Amazon with its Amazon Web Services solution, Microsoft with its Azure solution and Google through its Google Cloud solution.

As for big data, it refers to the treatment of large amounts of data, in which storage and processing models are used by which it seeks to find repetitive patterns that allow generating knowledge. In this sense, sensitive aspects of the use of Big Data are presented in the framework of public policies, in which security, data ownership, privacy and ethical framework of use are established as the main factor. From

this perspective, the immunity of cloud computing against attacks from all types of malware was affirmed a few years ago, however, this changed, demonstrating that no system is infallible and even less against DDoS. In fact, there is evidence of DDoS-type attacks and their taxonomy on cloud computing, as indicated by [43], in which they expose the types and various counter-attack measures (detection, prevention and tolerance techniques) for mitigate DDoS attacks.

Based on the foregoing, it is worth noting that when a cloud computing system is perpetrated, it is because the attacker has managed to gain access as administrator to one of the system nodes, so he can do whatever he pleases with the data by putting in serious trouble to its objective, in which it literally has in its hands the most important asset of an organization, which is information. These types of failures are usually attributed to human failures, either due to ignorance, negligence or complicity of the administrator or a worker.

The synergy of disruptive technologies such as IoT + Big Data + Cloub computing + IA allows the creation of an unparalleled technological infrastructure for the recording, analysis, processing and storage of massive data, where the intervention of the human being will be increasingly scarce. Taking into account that, in the following years the number of IoT devices will grow exponentially, the noted synergy will be increasingly robust and autonomous with a level of security that guarantees that the information is well protected. However, it is clear that DDoS attack techniques are also evolving, giving way to what can be called intelligent distributed denial of service (IDDoS), in which advanced algorithmic techniques of artificial intelligence are integrated to attack AI-based infrastructures.

7. Crytohacking

This type of attack is constantly growing, employing malware that has the ability to hijack cloud computing systems. It is aimed at large corporations and cryptocurrency exchange houses, using the computational power of mobile devices as an attack center, mining it with cryptocurrencies, making the user believe that they are rewarded under the assumption that they are carrying out large transactions under the blockchain model. In this context, crypto hacking resembles a DDoS attack with the difference that it not only hijacks computers, servers and web pages, but also smart mobile devices, which by mining them with cryptocurrencies can make fraudulent transactions at the cost of the victim, winning money secretly, since it is not possible to make a traceability with respect to the transactions that have been carried out. An example of malware with these characteristics is coinhive and cryptoMiner [44], discovered in multinational companies such as Tesla and Avira.

One problem that continues to grow is communication with anonymous networks and the Darknet (which involves the Deep web and the Dark web). This type of network, in principle, is intended to facilitate the access and flow of information in countries whose restriction of free expression does not allow open communication. However, this network is also used for criminal purposes which, as [45] points out, is used to commit computer crimes, share compromised files (personal, pornographic, confidential, illegal software, etc.) or for the sale of goods and services prohibited. The anonymity provided by the Darknet guarantees user navigation without any restriction compared to the conventional internet, so special browsers and protocols are required [46]. For this, it is common to use ".onion" extension that guarantees an anonymous IP to access the TOR network, or networks such as ZeroNet, FreeNet or I2P.

A peculiarity of the Darknet is that, although attacks are carried out from within, it shows itself to be highly flexible, dynamic and robust enough to adapt,

thus minimizing collateral damage, which is a notable differential characteristic with respect to the standard Internet. Based on this fact, when the Darknet is used for the purpose of hacking with cryptocurrencies, the probability of success is high because it operates under the blockchain model and distributed ledger [47]. This type of attack is in continuous growth parallel to ransomware, due to the ease of anonymously hijacking a device connected to the internet, added to the incessant increase in legal and illegal operations using the Blockchain as a cryptocurrency monetary system. For example, due to the particular technical and technological characteristics of the Darknet, it facilitates the exchange of sensitive information [48] between organized crime and terrorist groups, making it impossible for the authorities to intercept such as laundering. of money, planning and coordination of attacks, drug trafficking, tax evasion, hit men, kidnapping, extortion, child pornography, sale of weapons, etc.

Therefore, the combination of the blockchain with the Deep Web creates the ideal environment for the flow of legal or illegal information, in which it literally becomes almost impossible to trace [49], considering this cyberspace as a no man's land, where DDoS-type operations, among others, are carried out without any legal or police problem. Now, it should be noted that not only crime makes use of this type of network, but also government and military entities [50], institutions of higher education and research, among others, in which it seeks to guarantee anonymity and minimize risk of theft of critical information.

8. Ransomware

Ransomware is a type of cyberattack that is characterized by encrypting the files stored on a computer or web page by encoding them, where the victim must pay with cryptocurrencies for their ransom, which is why it is difficult to trace their origin or destination. This type of attack is constantly evolving in the way of encrypting information, using more sophisticated and robust algorithms that seek to hide the trail of the attacker, the form of payment and attacks on systems such as the cloud. As things are going, this type of attack will be more destructive and lethal, since it is combined with DDoS to enhance its level of hijacking, where the targets have been shifting from small companies to financial systems and industry, government and military structures and Critical infrastructures, which compromise their information and the operation of all their systems, paralyzing them, with the possibility of deleting or subtracting records and modifying them according to what the attacker or his contractor wants.

The ransomware only requires to hijack a few computers that are not updated in terms of security or to install itself by tricking its victims. Also, this malware (for example, Ekans) can be installed in SCADA-type systems [51] that are connected to the internet or to a local network whose security measures are deficient. What is critical about this type of attack is that it can be scalable, as long as the communication network infrastructure allows it, that is, when there is vulnerable software and hardware such as routers and other network devices. Also, other types of malware can be used to make way for ransomware, letting them carry out the tasks for which they were created and programmed, and then having the information as best suited. In this sense, the IoT with its various variants is not exempt from a ransomware-type attack, especially if the devices are being managed and/or administered by servers or mobile devices with an ephemeral degree of security.

The use of ransomware for targeted attacks (individuals or companies) is a great resource for organized crime, although at present it has diversified as it is a multi-platform malware, which allows it to affect Linux, Windows and MacOS operating

systems alike. For example, the Tycoon ransomware. That said, the attack can vary, encrypting personal or corporate files (web server, for example WastedLocker), locking the PC screen (lock screen), locking the hard drive and backups, blocking access to a mobile device, etc. The problem does not end here, since, at the time of the seizure of information, the attacker has unlimited access to the information, which allows the tracking of other potential victims, their computers and networks. An example that occurred in mid-2020 was through the Netwaklker malware, in which critical information was seized from the migration computer systems in the United States, which contained data from the Federal Intelligence Agency, some embassies and consulates, in which was asked for a ransom in the amount of 4 million dollars. It was not paid for it, but it exposed the vulnerabilities to which any system considered safe is found.

The ransomware attack feature consists of hiding it within files, which when executed by the victim installs a Trojan in the operating system, which internally begins to make changes to some registries, such as the keyboard, disables the anti-virus and any other program security, among other critical protection functions. The next step is to connect to the victim's network that is supposed to be vulnerable and enter via remote connection from the computer's desktop, which uses various protocols such as RDP (Remote Desktop Protocol) - Also, previously through social engineering, having guessed the password, but rather employ a brute force attack to find it. In general, there are a large number of tools to violate the system. Then, the process of encrypting files on the computer begins, including critical databases such as backups that correspond to servers -physical or in the cloud-, although more recently ransomware has been found that also encrypts data stored on network drives. Once the encryption is completed, the victim receives a message indicating immediate payment for the information seized through cryptocurrencies, otherwise it will be destroyed. Being able to decrypt ransomware is complex, especially since some of them already use symmetric encryption algorithms such as Galois/Counter (GCM) mode3 with a length of 16 bytes.

9. Artificial intelligence and advanced persistent threats

Although publications about cyberattacks using software based on artificial intelligence (AI) are scarce, it does not imply that they do not exist, since what is least wanted is publicity about it. AI can be used to find vulnerabilities in software such as hardware connected to a network, where appropriate equipment and resources are required for this purpose. For example, data can be searched on the darknet on activities related to clients or organizations that may be compromised and involve a security threat that is exploited by cybercriminals; this includes documentation and private information that has been infiltrated (personal and financial information, intellectual property, access credentials, etc.).

AI has already started to play a critical role when it comes to cybersecurity. Currently security companies use predictive models based on machine learning combined with neural networks and other disruptive technologies, in order to anticipate attacks on computer systems and critical infrastructures, as well as detect what is happening in a particular network. From this perspective, reverse engineering it to carry out attacks based on found vulnerabilities is viable, where robust datasets used as libraries can be used for brute force attacks. In fact, the creation of AI algorithms with programming that attacks certain systems already exists, the control of which is carried out by "intelligent" malware.

Although it is based on an assumption, with AI applied to carry out cyberattacks it compromises all the security of a system, including the lives of people and

society in general. An attack of this type would be planned to be executed on several fronts, using various resources such as advanced persistent threats (APT), DDoS, ransomware and other intelligent malware, hijacking certain critical systems, temporarily disabling them or destroying them, in such a way that any functionality or functionality collapsed. Operation of these in cyberspace, in this particular case of the different governmental and industrial organizations of a nation.

AI can not only threaten the security of an organization but that of any country, which can be orchestrated by organized criminal groups or by groups funded by governments and militia. An example of this are APTs, which are a highly specialized type of malware that is custom designed to infect and disable systems at the software and hardware level. The objective of this type of malware is the theft, modification, destruction, espionage and sabotage of industrial and corporate information. APTs possess stealth type attack traits, combining advanced encryption techniques with close polymorphic algorithms with AI. [52] points out that APTs can persist inside a computer system for a long time without being detected, taking advantage of the vulnerabilities of the infrastructure or the architecture of the communication protocols in the packaging of data in a network.

Based on the above, an APT is a cyber weapon designed for specific attacks on targets, particularly critical infrastructure. From this perspective, the IoT is no exception to an attack of this type, since communication between devices can be intercepted and disabled or modified. This is because APTs can leak through software or hardware that is not properly protected and from there scale the systems, so blocking or hijacking using a DDoS-type attack is feasible.

APTs are exclusive, so they are not abundant on the internet, this is because their managers are not just any organized criminal group, but governments, rival corporations and large criminal syndicates that have unlimited financial, technical and technological resources, which allows them undertake this type of development and carry out targeted cyberattacks. Under this model [53] point out that a variant of the APT called S-APT is used, whose action is focused on creating attack vectors based on disinformation strategies within the framework of the military.

The IoT within the framework of industry 4.0 increasingly incorporates AI in its developments, where connectivity to the internet and mobile devices is constantly increasing. Under this scenario, the introduction of an APT or malware similar to these technologies taking advantage of their vulnerabilities is feasible, either when they are already on the market or from their own manufacture, as demonstrated by [54]. Consequently, countless plausible scenarios are opening up to carry out cyberattacks, to and from drones, autonomous vehicles, advanced robots (military, industrial, leisure, etc.), smart electrical grids, even the IoT infrastructure that a smart city has. Consequently, the concern arises of programming errors in AI-based systems, which are exploited and taken advantage of to violate other systems, as demonstrated by the DeepXplore intelligent system [55].

10. Discussion from the bioethical plane

In the IoT industry, the term Edge Computing has recently been coined, which is the next step in Cloud Computing technology, in which all the information from intelligent IoT devices connected to a network is collected, to be stored and processed in large database repositories arranged for this purpose. The implications of this new proposal are broad and complex, because the data collected from sensors and various devices, combined with advanced AI algorithms, make inferences that lead to decision-making both human and automated devices. The density of data and its variety under this scheme will increase exponentially for the next few years,

exceeding zettabytes (10^{21} bytes), so technologies such as 5G, next-generation communication networks including the quantum internet, will accelerate and optimizing information traffic without saturating networks by reducing latency, incorporating other tools such as Edge/Fog Computing. It is worth mentioning that these technologies are characterized by the fact that the data is managed in the form of a chain of blocks or blockchain to guarantee a high level of security, which may possibly be migrated to specific applications such as the health field, minimizing the risk of compromising clinical information from the patients.

In the case of edge computing, it does not work alone apart from IoT, but is linked to other technologies such as Mobile Cloud Computing [56] and Collaborative Mobile Edge Computing [57], an example in this regard, are the Google Cloud IoT technologies, which are active in today's market. As they are considered as emerging technologies, the level of security is still in question, so the risk of compromising sensitive information of users and services through a crypto-hacking attack is high. Let us remember that the security infrastructure in the cloud is high, but not that of the IoT, added to the bad practices that inevitably lead to unauthorized access to a network.

Normally, unnecessary or insecure network services are activated, being exposed to attacks where unauthorized control of any service can be assumed, violating the confidentiality, integrity, authentication or availability of the information. Along the same lines, there are often interfaces that are managed by proprietary or third-party devices, such as mobile applications, data repositories in the cloud, the corporate website itself and the backend APIs. These flaws lead to vulnerabilities such as weak encryption (or lack thereof) on the data circulating on the network, as well as the absence of input/output filters.

Other common failures found in IoT devices are: failure to update firmware or manage related processes such as encrypting in transit and validating updates without appropriate mechanisms for doing so; 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 a formal permission or informed consent; absence of data encryption and access control.

There are variants of the IoT, such as the industrial and services field, known as the Internet of Robotized Things (IoRT), which is gaining strength due to the continuous industrialization that demands the attention of robots, particularly in industrialized countries. There is also the Internet of Things on the Battlefield (IoTotBF) [58]; which combines various advanced communication network technologies (including quantum ones) with massively interconnected systems, thus taking warfare to a new level of technicality. In this context, the technicality of the military is increasing and AI together with robotics are frequently used in the development of new intelligent weapons, of which there is no guarantee that something can go wrong in the field of cybersecurity. Viewed in this way as [59], oversight at the cybersecurity level by human operators is going to be increasingly difficult, if not impossible. This opens a strong discussion about the role of the human being in military operations, since the responsibility of decision-making is transferred to a machine about destroying a target in which it implies the death of innocents.

From the above, a number of questions are presented related to how to minimize the risk of a cyber-attack on a military infrastructure with technologies such as IoTotBF or similar, by foreign militias, terrorist groups, organized crime or by advanced automatic systems based on AI. We must not forget that the militias of various nations of the world are constantly developing new robotic and cybernetic technologies, aimed at improving their attack and defense systems while minimizing the number of casualties.

The IoT presents great benefits for society, as well as great challenges in terms of security, due to its integration with various standard and advanced communication technologies, which manage multiple devices in the home, industry, health and transportation, among others. This trend must be taken into consideration not only by manufacturers and governments, but by society itself, since the risk of information collection by third parties is high and the uncertainty of its handling remains between said. In fact, the tradeoffs of transparency in the management of information by governments and large corporations are critical, and this problem will be further accentuated with the advent of next generation technologies.

As for cyberattacks such as DDoS combined with other techniques mentioned throughout the chapter, the spectrum of damage to private and public computer networks is broadened, including devices connected to it such as the IoT, mobile devices and other emerging technologies. In this sense, the authorities and governments in general must take the potential cyberattacks that can be carried out on critical infrastructures such as health very seriously, since not only information is compromised, but people's lives are compromised. For example, zero-day or volume-based DDoS attacks, which are difficult to avoid due to the speed with which they run. In fact, it only takes one flaw for a botnet to saturate its target's network and fully control it. Along the same lines, there are other types of more sophisticated, highly destructive and selective attacks that take control of a system, such as protocol attacks, in this case TCP directed at networks that communicate with servers, firewalls (physical and logical), gateways and load balancers, where damage to an infrastructure can be severe.

To recap, although the attacks mentioned in this document are attributed to organized groups, a person with minimal knowledge could put an institution, industry and even a nation in serious trouble, since some of the information to create malware does not It is only found on the Darknet, but on the conventional internet, where with a minimal payment you can find programs to create ransomware and other types of computer viruses. Likewise, you can hire the service of any type of malware, the packages are sold on the dark web for reasonable prices, even malware kits. Most of the public is unaware of this type of thing and in this way is exposed to their personal or corporate information being stolen by cybercriminals.

Based on what is stated in this document, it is evident that special attention must be paid to privacy, ethical, bioethical and legal aspects, security and rights, among other elements that threaten human dignity. Under this fact, there is a constant concern about the unauthorized access and manipulation of personal and massive data concentrated in technologies such as big data, IoT, cloud computing, among others, which contain sensitive information at a clinical, ethnic, sociocultural, economic, financial and industrial, etc., which require a thorough examination from the bioethical and biopolitical point of view that guarantee respect for the protection of information. At this point, a number of elements arise to evaluate, because not only is reference being made to the seizure of information and sale of it to third parties, but also to irreparable damage to the individual in terms of inequity or damage generated by the interference to the private life of the victim or victims.

Under the exposed characteristics of a cyberattack, the violation in terms of property, rights, use, exploitation, maintenance and licenses for the administration of massive data, means little or nothing for the attackers, but if a great legal, ethical weight, bioethics and security for the organization and/or personnel in charge of managing and administering this data. From this point of view, there are gray areas regarding the formulation of public policies that guarantee an adequate safeguard on the property of the data, protection and prohibition of use for other purposes, so it is expected that in the coming years letters will be taken on this matter will

require the collaboration of various groups of experts and disciplines that seek to minimize risks, both in the handling of massive data, and in cyberattacks by various means.

11. Conclusions

Society is increasingly dependent on technology, examples of which are: the internet, mobile technology, artificial intelligence, big data, cloud computing and blockchain among others, which facilitate the management and administration of massive information. In the case of the IoT, it has been becoming widespread in various environments such as health, industrial, transport and services, among others, progressively incorporating the aforementioned technologies. In this sense, there is growing concern about the fragility of this technology, which proves to be notoriously vulnerable to cyberattacks. The reason for this is the continuous proliferation of IoT devices that do not meet the minimum-security standards; thus, they expose an individual and society in general to being spied on and possibly attacked. Added to this panorama are the vulnerabilities inherent to communication architectures, which have yet to be resolved, and the lack of management and administration of devices by the personnel in charge, which increase the risk of unauthorized access to an information system. What is critical about this matter is that the health sector has been incorporating the IoT into its services and although it takes their security very seriously, the spectrum of vulnerabilities to which this technology is subjected is alarming.

The IoT is expanding its range of action by integrating with 5G communication networks, and the hospital environment is no stranger to this. With this in mind, the diversification of services and connectivity will be reflected in Smart City, Green Systems and Transport Systems, which will facilitate the analysis and visualization of large volumes of data that the IoT generates permanently. This implies that secure communication architectures are required, capable of withstanding attacks of various kinds, particularly those of the DDoS type that have been expanding their modalities by integrating other advanced malware technologies. Consequently, the development of networks of sensors, actuators and remote diagnostic systems will require a unification of standards and protocols that guarantee that the IoT devices that are or are released on the market present a minimum risk that compromises critical or sensitive information, well of a person, institution, industry or government.

Based on the current global instability attributed to social, political, economic, health and environmental factors, cyberattacks have not diminished. In fact, with the problem of the COVID-19 pandemic, remote work skyrocketed and with it the objectives of cybercriminals were diversified, where resources such as corporate VPN gateways and non-public web resources such as emails have been compromised by the high risk of being hijacked by malware, such as APTs, ransomware and botnet, to name a few, giving way to the growth of the DDoS market.

Finally, in the coming years an increase in IoT devices is predicted in large cities in their critical infrastructures, expanding their services and promoting permanent monitoring in search of anomalies of various types: climate, environmental pollution, security (citizen, computing, biosafety, etc.), mobility and health, among others, which is why the use of other technologies for the analysis and treatment of massive data is expected to explode, and with it the risk and vulnerabilities that need to be addressed from now on. The task in this sense is not easy but it is not impossible either, technologies such as quantum encryption, quantum internet and AI processors that reduce the risk of attacks on hardware such as system software,

are some advances that promise to reduce the gap to information security. However, there is a problem regarding the role that governments play under what is stated in this document, since in the end their transparency in the handling of information is debatable, especially when it has an incalculable value.

Conflict of interest

The author declares no conflict of interest.

Author details

Jairo Eduardo Márquez Díaz
Universidad de Cundinamarca, Chía, Colombia

*Address all correspondence to: jemarquez@ucundinamarca.edu.cor

References

[1] Ozturk, T., Talo, M., Yildirim, E. A., Baloglu, U. B., Yildirim, O., & Rajendra, A. U. Automated detection of COVID-19 cases using deep neural networks with X-ray images. Computers in Biology and Medicine, 2020, 103792. Advance online publication. https://doi.org/10.1016/j.compbiomed.2020.103792

[2] Jiang, X., Coffe, M., Bari, A., Wang, J., Jiang, X., Huang, J., et al. Towards an Artificial Intelligence Framework for Data-Driven Prediction of Coronavirus Clinical Severity. Computers, Materials & Continua (CMC). 2020, 63(1). 537-551. http://doi.org/ 10.32604/cmc.2020.010691

[3] Adam, M., Wessel, M., & Benlian, A. AI-based chatbots in customer service and their effects on user compliance. Electronic Markets. 2020. http://doi.org/10.1007/s12525-020-00414-7

[4] Mäki, P., Rauti, S., Hosseinzadeh, S., Koivunen, L., & Leppänen, V. Interface diversification in IoT operating systems. Proceedings of the 9th International Conference on Utility and Cloud Computing - UCC '16. 2016. doi:10.1145/2996890.3007877

[5] Mahjabin, T., & Xiao, Y. Mitigation Process for DNS Flood Attacks. 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2019. http://doi.org/10.1109/ccnc.2019.8651715

[6] Abdmeziem, M., Tandjaoui, D. & Romdhani, I. Lightweighted andenergy-aware mikey-ticket for e-health applications in the context ofinternet of things. International Journal of Sensor Networks, 2018, 26(4), 227-242.

[7] Hao, H., Wang, Y., Shi, Y., Li, Z., Wu, T & Li, C. IoT-G: una arquitectura de comunicación inalámbrica de energía privada de baja latencia y alta confiabilidad para redes inteligentes. IEEE International de 2019 Conferencia sobre tecnologías de comunicaciones, control y computación para redes inteligentes (SmartGridComm), Beijing, China, 2019, 1-6, doi: 10.1109/SmartGridComm.2019.8909773.

[8] Ejaz, W., Anpalagan, A., Imran, M. A., Jo, M., Naeem, M., Qaisar, S. B., & Wang, W. Internet of Things (IoT) in 5G Wireless Communications. IEEE Access, 2016, 4, 10310-10314. doi:10.1109/access.2016.2646120

[9] Acharya, S. & Tiwari, N. Survey of DDoS Attacks Based On TCP/IP Protocol Vulnerabilities. OSR Journal of Computer Engineering (IOSR-JCE), 2016, 18(3), 68-76. http://doi.org/0.9790/0661-1803046876

[10] Alotaibi, A. M., Alrashidi, F. B., Naz, S. & Parveen, Z. Security issues in protocols of TCP/IP Model at Layers Level. International Journal of Computer Networks and CommunicationsSecurity, 2017, 5 (5), 96-104

[11] Elejla, O. E., Anbar, M., & Belaton, B. ICMPv6-Based DoS and DDoS Attacks and Defense Mechanisms: Review. IETE Technical Review, 2016, 34(4), 390-407. doi:10.1080/02564602.2016.1192964

[12] Santiago, A. et al. Modelo de Seguridad para Garantizar la Integridad de Pagos Móviles sobre Near Field Communication (NFC). Rev. Espacios, 2018, 39(19), 6-30.

[13] Márquez, D. J. Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas. Revista Biòtica i Dret. Rev Bio y Der. 2019; 46: 85-100. https://doi.org/10.1344/rbd2019.0.27068

[14] NSA and FBI. National Security Agency Federal Bureau of Investigation

Cybersecurity Advisory. Russian GRU 85th GTsSS. Deploys Previously. Undisclosed Drovorub Malware. Rev 1.0, U/OO/160679-20, PP-20-0714.

[15] Coffey, K., Smith, R., Maglaras, L., & Janicke, H. Vulnerability Analysis of Network Scanning on SCADA Systems. Security and Communication Networks, 2018, 1-21. doi:10.1155/2018/3794603

[16] Rose, K., Eldridge, S. & Chapin, L. La internet de las cosas - Una breve reseña para entender mejor los problemas y desafíos de un mundo más conectado, Internet Society (ISOC). Available June 10, 2020: https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf

[17] Barrio, A. M. Internet de las cosas. Madrid, España, 2018, Editorial REUS.

[18] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K. and Zhou, Y. Understanding the mirai botnet. 26th USENIX Security Symposium. Vancouver, BC: USENIX Association, 2017, 1093-1110.

[19] Kupreev, O., Badovskaya, E. & Gutnikov, A. Ataques DDoS en el primer trimestre de 2020. Available June 13, 2020: https://securelist.com/ddos-attacks-in-q1-2020/96837/

[20] Márquez, D. J. Seguridad metropolitana mediante el uso coordinado de Drones. Ingenierías USBMed, 2018, 9(1), 39-48. http://doi.org/10.21500/20275846.3299

[21] Nardi, D. Country update: China. Religious Freedom in China's High-Tech Surveillance State. Washington, DC., United States of America, United States Commission on International Religious Freedom (USCIRF), 2019.

[22] Bignami, F. Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance. GWU Law School Public Law Research, 2018, 1-20.

[23] Lemieux, F. Intelligence and state surveillance in modern societies: an international perspective. Howard House, United Kingdom, Emerald Publishing Limited, 2019.

[24] Feliu, R. J. Smart Contract: Concepto, ecosistema y principales cuestiones del Derecho privado. In: La Ley mercantil: Contratación mercantil, 47, ed. Wolters Kluwer, 2018, 7-10.

[25] Alharby, M. & Moorsel, A. Blockchain-based smart contracts: a systematic mapping study. Computer Science & Information Technology, 2017, 125-140. http://doi.org/ 10.5121/csit.2017.71011

[26] Savchenko, V. Detection of Slow DDoS Attacks based on User's Behavior Forecasting. International Journal of Emerging Trends in Engineering Research.2020, 8. 2019-2025. 10.30534/ijeter/2020/90852020.

[27] Rashidi, B., Fung, C. CoFence: a collaborative DDOS defence using network function virtualization. In: 12th International Conference on Network and Service Management (CNSM 16), October 2016.

[28] Hosseinzadeh, S., Hyrynsalmi, S., & Leppänen, V. Obfuscation and diversification for securing the internet of things (IoT). Internet of Things, 2016, 259-274. doi:10.1016/b978-0-12-805395-9.00014-9

[29] Wang, M., Lu, Y. & Qin, J. A Dynamic MLP-Based DDoS Attack Detection Method Using Feature Selection and Feedback. Computers & Security, 2019, 1-15. https://doi.org/10.1016/j.cose.2019.101645

[30] Zekri, M., Kafhali, S. E., Aboutabit, N., & Saadi, Y. DDoS attack detection using machine learning techniques in cloud computing environments. 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), 2017. http://doi.org/10.1109/cloudtech.2017.8284731

[31] Aljumah, A. Detection of Distributed Denial of Service attacks using artificial neural networks. (IJACSA) International Journal of Advanced Computer Science and Applications, 2017, 8(8), 306-318.

[32] Zhang, B., Zhang, T., & Yu, Z. DDoS detection and prevention based on artificial intelligence techniques. 2017 3rd IEEE International Conference on Computer and Communications (ICCC), 2017. doi:10.1109/compcomm.2017.8322748

[33] Innus, M. D., Simakov, N. A., Jones, M. D., White, J. P., Gallo, S. M., DeLeon, R. L., & Furlani, T. R. Effect of Meltdown and Spectre Patches on the Performance of HPC Applications. 2018. arXiv preprint arXiv:1801.04329

[34] Giles, M. Estos han sido los peores ciberataques en lo que llevamos de 2018. [Internet]. 2020. MIT Technology Review, Available from: https://www.technologyreview.es/s/10339/estos-han-sido-los-peores-ciberataques-en-lo-que-llevamos-de-2018 [Accessed: 2020-june-14]

[35] Metcalf, D., Milliard, S. T. J., Gomez, M., & Schwartz, M. (2016). Wearables and the Internet of Things for Health: Wearable, Interconnected Devices Promise More Efficient and Comprehensive Health Care. IEEE Pulse, 7(5), 35-39. doi:10.1109/mpul.2016.2592260

[36] Spender, A., Bullen, C., Altmann-Richer, L., Cripps, J., Duffy, R., Falkous, C., ... Yeap, W. (2019). Wearables and the internet of things: considerations for the life and health insurance industry. British Actuarial Journal, 24. doi:10.1017/s1357321719000072

[37] Qureshi F. & Krishnan, S. (2018). Wearable Hardware Design for the Internet of Medical Things (IoMT). Sens Basel. 18(11):3812

[38] Rodríguez, G. R. (2019). Internet de las cosas: Futuro y desafío para la epidemiología y la salud pública. Universidad Y Salud, 21(3), 253-260. https://doi.org/10.22267/rus.192103.162

[39] Tao, H., Bhuiyan, M. Z. A., Abdalla, A. N., Hassan, M. M., Zain, J. M. and Hayajneh, T. (2019). Secured Data Collection with Hardware-Based Ciphers for IoT-Based Healthcare. IEEE Internet of Things Journal, vol. 6, no. 1, pp. 410-420, Feb. 2019, doi: 10.1109/JIOT.2018.2854714.

[40] Elkhodr, M., Alsinglawi, B. & Alshehri M. (2019) A Privacy Risk Assessment for the Internet of Things in Healthcare. In: Khan F., Jan M., Alam M. (eds) Applications of Intelligent Technologies in Healthcare. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-319-96139-2_5

[41] Alraja, M. N., Farooque, M. M. J. & Khashab, B. (2019). The Effect of Security, Privacy, Familiarity, and Trust on Users' Attitudes Toward the Use of the IoT-Based Healthcare: The Mediation Role of Risk Perception. IEEE Access, 7,111341-111354, doi: 10.1109/ACCESS.2019.2904006.

[42] Thibaud, M., Chi, H., Zhou, W., & Piramuthu, S. (2018). Internet of Things (IoT) in high-risk Environment, Health and Safety (EHS) industries: A comprehensive review. Decision Support Systems, 108, 79-95. doi: 10.1016/j.dss.2018.02.005

[43] Qureshi F. & Krishnan, S. (2018). Wearable Hardware Design for the

Internet of Medical Things (IoMT). Sens Basel. 18(11):3812

[44] Deshmukh, R. V., & Devadkar, K. K. Understanding DDoS Attack & its Effect in Cloud Environment. Procedia Computer Science, 2015, 49, 202-210. http://doi.org/10.1016/j.procs.2015.04.245

[45] Eskandari, S., Leoutsarakos, A., Mursch, T., & Clark, J. A First Look at Browser-Based Cryptojacking. 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). 2018, 58-66. http://doi.org/10.1109/eurospw.2018.00014

[46] Arenas, A. La resiliencia de la red oscura. Un estudio logra describir las propiedades estructurales de la «Internet invisible» y explica por qué esta se muestra tan inmune a los ataques informáticos. Rev. Investigación y Ciencia, 2018, 498, 12-14.

[47] Beshiri, A. S. and Susuri, A. Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review. Journal of Computer and Communications, 2019, 7, 30-43. https://doi.org/10.4236/jcc.2019.73004

[48] Lipton, A. & Pentland, S. Hacer saltar la banca. Investigación y Ciencia, 2018, 498, 16-23.

[49] Mirea, M., Wang, V., & Jung, J. The not so dark side of the darknet: a qualitative study. Security Journal, 2018. doi:10.1057/s41284-018-0150-5

[50] Bautista, D. L. Deep web: aproximaciones a la ciber irresponsabilidad. Revista Latinoamericana de Bioética, 2015, 15(1), 26-37.

[51] Chertoff, M. A public policy perspective of the Dark Web. Journal of Cyber Policy, 2017, 2(1), 26-38. doi:10.1080/23738871.2017.1298643

[52] Ibarra, J., Javed Butt, U., Do, A., Jahankhani, H., & Jamal, A. Ransomware Impact to SCADA Systems and its Scope to Critical Infrastructure. 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3). doi:10.1109/icgs3.2019.8688299

[53] Márquez, D. J. Armas cibernéticas. Malware Inteligente para ataques dirigidos. Ingenierías USBMed, 2017, 8(2), 48-57. http://doi.org/10.21500/20275846.2955

[54] Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack. Computers & Security, 2019. doi: 10.1016/j.cose.2019.07.001

[55] Choi, C. Q. Lo siento, Dave. Rev. Investigación y Ciencia, 2018, 499, abril, p. 8.

[56] Pei, K., Cao, Y., Yang, J. & Jana, S. DeepXplore: automated whitebox testing of deep learning systems. Communications of the ACM. 2019, 62. 137-145. http://doi.org/10.1145/3361566.

[57] Tran, T., Hajisami, A., Pandey, P. & Pompili, D. Collaborative mobile edge computing in 5g networks: new paradigms, scenarios, and challenges. IEEE Commun Mag, 2017, 55(4), 54-61.

[58] Márquez, D. J. Nanotecnología. Internet de las cosas. [Internet]. 2019. Available from: http://doi.org/10.13140/RG.2.2.33697.66402 [Accessed: 2020-oct-04]

[59] Theron, T. P. et al. Towards an Active, Autonomous and Intelligent Cyber Defense of Military Systems: the NATO AICA Reference Architecture. International Conference on Military Communications and Information Systems, Warsaw, Poland, 22nd - 23rd May 2018.