Forensic challenges regarding the Internet of Things

Ancuța Elena Franț

1 Faculty of Law, Alexandru Ioan Cuza University of Iași, Romania

Abstract. The Internet of Things brings many benefits to our society, but its advantages come with a price, namely with a huge opportunity for those who want to commit cybercrime. To fight against this kind of criminality, investigators must use appropriate methods. The Forensics of the Internet of Things (IoT) has evolved from “traditional” Digital Forensics, and includes, among other activities, the identification of the devices related to a certain crime, collecting the digital evidence in a form which can be used in front of the judicial bodies, the analysis, and the extraction of all possible information from the collected data, and the preservation of the evidence. The Forensics of IoT must face specific issues, mainly generated by the extraordinary large number of IoT devices and by the great diversity of these devices. An important problem is that data analysis is very difficult to perform, because of different data formats used by the components of IoT. In the forensic investigations related to the IoT, an important concern refers to privacy protection. Overall, IoT Forensics is a challenging field, but we must search for suitable solutions, because ensuring security for IoT is a very important aim.

1 Introduction. The importance of a forensic approach to the Internet of Things

The present-day society is becoming more and more dependent on the Internet. This situation is generated by the great advantages which come along with the use of the Internet. People see their lives greatly enhanced with online services, in all areas. But all this comes with a price. The characteristic features of the Internet have made it an appropriate environment for anti-social activities. From fraud to threat, from sexual abuse to blackmail and drug trafficking, an immense variety of crimes can be committed through internet. The possibility for the perpetrators to easily hide their identity and the difficulties which may arise in the criminal investigations, along with the huge potential profits, all are highly tempting for many people, who decide to get involved in criminal activities using the Internet [1], [2].

Among the benefits which are brought in by the Internet, a great part of them is obtained through the Internet of Things (abbreviated IoT). The great importance of this field appears to be obvious, when we think that the IoT literally surrounds us, from the moment we wake up till we go asleep. Even more, we dare to assert that the IoT continues to accompany us while we are sleeping, as lots of devices connected to the Internet continue to function while we are asleep. This area of the Internet has some specific features, which require specific investigation methods.

* Corresponding author: ancuta.frant@uaic.ro
when a crime has been committed in this field. The specificity of the investigation’s techniques and tactics is very important, to have real chances to find the criminals.

Essentially, we aim to highlight the most important aspects regarding forensic methodology applied in cases where the IoT is somehow linked to a crime that has been committed. To reach our goal, we will first present what IoT means and what place it occupies in the Internet universe.

1.1 Methodology

In this paper we will present the results that we have achieved through a systematic literature review regarding the meaning of the IoT and the specificity of forensic methodology used in investigating crimes related to the IoT. We will emphasize the difficulties which can be encountered in the criminal investigations regarding IoT, as well as the differences between the so-called “traditional” Digital Forensics and the Forensics used when criminality is related to the IoT. We will analyse the results and we will draw conclusions in refer to the forensic challenges regarding the IoT.

1.2 Results

The order in which we choose to present the information we have found is determined by the desire to make a clear presentation of the topic under discussion. Thus, at the beginning we will present the information necessary to understand what the IoT is, highlighting the characteristic aspects of this field. Knowing the specifics of the IoT is a prerequisite to understanding the features of the IoT Forensics, features that clearly distinguish it from other forensic domains.

2 Defining the Internet of Things

Explained in a simple manner, the Internet of Things (IoT) is a concept that defines a world where all objects (cars, household appliances, lighting systems, mobile devices etc.) are connected to each other through the Internet or another communication network. The IoT is not only based on computers to exist. Each object, and even the human body, can become a part of IoT if equipped with certain electronic components. The objects which are a part of the IoT must fulfil two conditions: 1.) the object must be able to capture data, usually through sensors; 2). the object must be able to transmit this data elsewhere through the Internet or through another network [3]. According to industry analysts, in the year 2019 there were approximately 8.6 billion IoT devices and, at the end of the year 2022 and in the beginning of the year 2023, there are approximately 13.1 billion IoT devices, with 130 new devices connecting every second. Experts forecast that, in the year 2030, there will be approximately 30 billion connected devices in the IoT network [4], [5].

It is important to highlight that, although the name of the field is Internet of Things, the concept refers to the devices connected through a network, which may or may not be the Internet [6].

Basically, the IoT is a huge network of connected devices which collect and analyse data and perform different tasks in an autonomous manner. The great development of IoT has been facilitated by the improvement of communication technologies (like 5G) and data analysis systems (which use Artificial Intelligence – AI and Machine Learning). All these elements bring a high connectivity and a precise ability to collect and to analyse data, in real time. This enables IoT to apply for a great category of objects, from light, wearable ones (smartphones, smartwatches) to smart cars, smart city infrastructure and smart public utilities (leading to the so-called “smart cities”) and industrial equipment [5]. Also, smart services have greatly benefited from IoT. IoT has virtual limitless possibilities, as it can be implemented for an extremely high
range of purposes, sometimes in surprising areas. For example, IoT is being used in agriculture, leading to the so-called “smart agriculture”. In this domain, IoT applies by monitoring the fields with dedicated sensors, which indicate exactly how much watering and fertilization is needed, depending on the data gathered about a certain field. This helps to obtain better crops, as well as leading to a sustainable agriculture, as water and fertilizers are not wasted, but used only when they are needed [5]. Also, IoT is already used for pollution control, energy saving, smart transportation, and smart industries [7]. Even electronic cigarettes can be a part of the IoT. Overall, it seems that nothing can be surprising in the IoT era, and we can expect that IoT is applied in areas we could have never thought it could be used.

But how did it all begin? The use of connected devices which gather and analyse data in real-time has been a reality for a few decades before the exponential growth of the IoT. For example, smart alarm cars, coordinated traffic lights, electronic wristwatches (to monitor heartbeat) have been in use for some time now [5]. The first encouraging results obtained through such devices certainly determined people to obtain even more benefits. This desire has been also fuelled by favourable conditions, like the evolution of technology and the decrease of the costs of the components. In the evolution of the IoT, researchers have identified three generations: “the first one of tagged objects; the second one of things interconnection through web technologies; the third one of social objects, semantic data representation, and cloud of things” [8].

In search of a definition for the IoT, it is important to pay attention to the definitions given by official authorities. This is why we want to mention the definition given by the European Parliament, which states that “The Internet of Things (IoT) refers to a distributed network connecting physical objects that are capable of sensing or acting on their environment and able to communicate with each other, other machines, or computers. The data these devices report can be collected and analysed to reveal insights and suggest actions that will produce cost savings, increase efficiency, or improve products and services.” [9]

It is important to mention that, in some papers, there are specific views (and, hence, definitions), about some elements of the IoT. For example, in the Report from the Commission to the Council and the European Parliament: Final report - sector inquiry into consumer Internet of Things, “smart devices” are defined as “wireless electronic consumer Internet of Things devices, such as wearable devices, smart speakers and other smart home devices, capable of connecting to other devices or networks, exchanging data with them, and operating to some extent interactively and autonomously. This definition does not include smart mobile devices (i.e., smartphones and tablets)” [10]. We notice that, in this report, the term “smart device” has a narrower meaning that it is usually understood.

The term Internet of Things has been linked to various concepts and technologies, and sometimes the use of the term has not been very precise. Some authors show that “in spite of its huge success, what IoT really represents is not completely clear” [8]. The evasive meaning associated by some authors with the IoT (especially in the beginning of its use, but not only then) may imply that it is possible that there is a widespread misunderstanding regarding the meaning of the concept. Some authors point out that the IoT is just related to Radio frequency identification system (RFID), while others believe it is a web of sensors. Also, some consider that IoT is a sort of Machine-to-Machine communication. Although there is not a unanimous understanding of the IoT, industry takes benefits from the popularity of IoT, due to its solution-oriented profile, which makes it very appropriate to the consumer market. Overall, the scientific literature does not bring much in terms of clarifying the meaning of IoT, as authors offer definitions which are often in discordance [8]. A first step to clarify the significance of the IoT is to understand the differences between IoT and other similar terms.
3 Separating the Internet of Things from similar concepts

The IoT is similar to other concepts, and, in the following lines, we will present some of these concepts, namely Internet, Machine to Machine (M2M), Industrial Internet, Industrial Internet of Things (IIoT), Web of Things, Internet of Everything (IoE).

**Internet** is defined by the fact that connections are only made between people, but this simple assertion does not cover all the implications of the Internet. However, the simplicity of such a definition helps to understand what Internet means in opposition to other similar concepts. In the scientific literature there is not unanimity regarding the definition of the Internet. Many authors present the Internet in material terms, as a combination of hardware and software, and see the evolution of the Internet as the spread of these technologies, in space and time. Some authors argue that it is not a problem that many definitions exist but warn that “historians should be aware of the politics of the definitions they use” [11].

**Machine to Machine (M2M)** communication is a communication technology defined by the fact that many smart devices can “autonomously communicate with each other and make collaborative decisions without direct human intervention” [12].

**Industrial Internet** refers to the integration and linking of big data, analytical tools, and wireless networks with physical and industrial equipment [13]. Industrial Internet “is a promising technology combining industrial systems with Internet connectivity to significantly improve the product efficiency and reduce production cost by cooperating with intelligent devices, in which the advanced computing, big data analysis and intelligent perception techniques have been involved” [14]. Unlike Machine to Machine, the Industrial Internet includes not only the connections between machines, but also human interfaces [3].

**Industrial Internet of Things (IIoT)** “refers to the use of smart sensors, actuators, fast communication protocols, and efficient cybersecurity mechanisms to improve industrial processes and applications” [15].

**Web of Things (WoT)** is a concept which refers to the possibility that everyday objects are fully integrated with the Web [16].

**Internet of Everything (IoE)**, although a rather vague concept, refers to all connections that can be imagined, between people, things, data, and processes, with the purpose to offer better experiences and to lead to smarter decisions. The IoE promises to bring fundamental changes to our lives, redefining the way we interact, the way we work, along with a wide range of other benefits [17].

4 The deeper meanings of the term Internet of Things

The term **Internet of Things** has been first officially used by Kevin Ashton. He used it as a title of a presentation he made at Procter & Gamble (P&G), in 1999. Through this term, Ashton referred to the network which connects people and objects around them. As it can be seen from the previous information in this article, in the present day, the term is often defined by letting apart the human factor, as it roughly points out to the connection between objects. It is important to say that, in the vision of its creator, the term **Internet of Things** has a slightly different meaning, as we will further show [18].

In 2009, ten years after Ashton first used the term, he highlights that, when he referred to the **Internet of Things** in 1999, he wanted to point out that computers (and other technical devices) need to grow their independence from humans in what regards data collection. He had noticed, at the time when he first used the term, that computers, smart devices, and Internet itself were all depending on humans. In other words, all the information existing on the Internet was, somehow, created by human beings (for example, by taking a picture, typing a letter, or pressing a button). Ashton pointed out that humans are not very good at collecting data, because of specific human features (they don’t have enough attention or precision) and/or because they do not have very
much time at their disposal to dedicate it to gathering information complex enough. It is normal for people to not be able to pay enough attention to recording data or to analyse ideas, because real human life and society are based on things, not on information or ideas. In an eloquent example, Ashton points out that humans cannot survive by eating bits or use them as fuel. This is why Ashton expressed his desire that computers become less dependent on people in the process of collecting data. Through this, Ashton believes that we could “reduce waste, lost and cost” [18].

Ashton notices that, ten years after the first use of the term Internet of Things, great improvement has been made in empowering computers to gather data by themselves. Now, computers have a very good understanding of the world, without help from humans. But, still, we must deepen our knowledge about what computers can do. Kevin Ashton confidently states that “The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so.” [18]

Furthermore, it is not only about what computers can do, but also about the future implications of the growing Internet of Things. The impact is so great, that the European Commission launched a consumer IoT inquiry in 2020, as part of the European Commission digital strategy. The purpose of this inquiry was to obtain a better understanding of what does the consumer IoT mean, how does competition work in this domain and what problems may arise concerning competition, and which are the directions of evolution for the consumer IoT. In the final report of this inquiry, published in 2022, it is stated that a growing number of devices and services are becoming part of the IoT and that “overall consumer IoT revenue worldwide will grow from EUR 105.7 billion in 2019 to approximately EUR 404.6 billion by 2030” [10].

5 The insights of the Internet of Things

The IoT creates many business opportunities. Many of these opportunities are only known to experts in this domain. Usually, the mass media focus attention on the part of the IoT dedicated to the consumer. There is no doubt that products dedicated to the consumer have an important place in the IoT, but they are only a part of it. Studies indicate that IoT has a lot to offer even to businesses for which, apparently, the IoT doesn’t have much to offer. The IoT has the potential to create important effects on every business activity, regardless the industry type. IoT can solve many problems that businesses have been facing for decades. Along with other technological developments (for example, cloud computing, smart grids, nanotechnology, and robotics), the IoT brings a significant contribution to achieving an economy characterized by increased efficiency, productivity, safety, and profit [3]. Overall, IoT has transformed the traditional way of living into something we can call “a high-tech lifestyle” [7].

We can say that, now, the IoT is no longer an isolated IT segment, but an important factor which sustain much of the world’s economy. The number of industrial activities that are not influenced by the IoT is very small, and the number of industries in which the IoT is vital for performing the specific activities is increasing [3].

Furthermore, favourable conditions must be created in what concerns the radio spectrum, meaning that it must be allocated the needed radio spectrum, in accordance with the rapid growth of the IoT. This is because Radio frequency identification system (RFID) is extremely important in the functioning of the IoT. RFID is an automatic technology which helps computers to “identify objects, record metadata or control individual target through radio waves” [19]. By connecting RFID reader to a certain terminal of the Internet, “the readers can identify, track and monitor the objects attached with tags globally, automatically, and in real time (...)” [19].

According to a study conducted by the Pew Internet Project Research, 83% of technology experts and users of the Internet agree with the idea that the IoT will have widespread benefits by 2025 [3]. The European Parliament asserts that the IoT can thus bring key contributions to implementing the European Union strategy for “smart, sustainable and inclusive growth” [9].
6 The essential elements of the Internet of things

Knowing the essential elements which make IoT work is important in our quest, because it allows us to better understand the risks that threaten IoT, and, further, the challenges of the IoT Forensics. This is why we will describe, in short, the essential elements involved in the functioning of the IoT.

Distributivity refers to the fact that the IoT works in a highly distributed environment, meaning that data is collected from different sources (the devices) and processed by several entities in a distributed manner [3].

Interoperability means that devices from different vendors need to cooperate to achieve the common goals. Systems and protocols must be designed in a way that allows devices made by various manufacturers to exchange data [3].

Scalability refers to the fact that the IoT is made up by billions of objects, which means that the systems and applications running on top of the network will have to manage huge amount of data [3].

Resource deficit in IoT means that both energy power and computing resources are extremely limited [3].

Security issues may arise in the IoT, which can be an impediment for some potential users to buy devices included in the IoT [3].

7 The risks faced by the Internet of Things

All opportunities offered by the IoT are linked to a certain level of risk, and, in what concerns IoT, the risks are as important as the rewards. Any object in the IoT world is an entry point through which cybercriminals can penetrate the system. This is why businesses cannot afford to enter the IoT unprepared [3].

As specialists state, the IoT brings major challenges to the human society. An important issue is related to ensuring wide choice opportunities for consumer, and this can be achieved by encouraging competition. Also, innovation must be sustained, because it can bring new technologies, which may be easier to use or may bring greater security. Open standards must be adopted, to offer equal opportunities to all the players in the market [9].

Security comes out as a major concern related to the IoT, because the large number of connected objects makes it easy to steal personal data and use it in illegal purposes. Overall, to enhance the benefits and to reduce the risks of the IoT, a balance must be kept between people’s privacy rights and the gains which can be obtained through the IoT [9].

In a world where machines are starting to replace people and become decision makers, and sensors capture data continuously, questions arise regarding security guarantees, as cyberattacks can seriously affect privacy. Studies point out that the IoT has an impact in every country and economy on planet, even in the developing world. Therefore, appropriate measures are required, especially due to the increasing role which IoT has for industries, as well as for consumers [3].

Some authors bring into discussion another risk related to the IoT. This risk may arise from a poor understanding of the meaning of the IoT, fuelled by the fact that, as we have pointed out before, there is not an unanimously accepted definition of IoT. If the IoT domain is poorly understood (in reference to its meaning, to its technologies, its purposes etc.), IoT may end up being mistrusted by its potential users, which will decrease its application in the human society [8], at least when it comes to consumer IoT.

Studies point out that, usually, IoT is threatened by malware, including ransomware; botnets and Distributed Denial-of-Service (DDoS) attacks; data theft. The phishing attacks are the cause of nine out of ten data breaches [20].

Overall, some specific features of the IoT, like wide distribution and openness, make IoT an ideal target for cybercrime [21]. This is why efficient methods must be taken, to properly respond
to the severity of the cyberattacks. The urge for high security in IoT becomes even more clear as studies point out that IoT devices are usually attacked within five minutes after they have been connected to the Internet [22].

8 The purpose of IoT Forensics

As a response for the risks confronted by the IoT, a first step is to take protective measures against such risks (which makes the object of IoT security, a distinct scientific field). However, in some cases, such measures do not work, due to various reasons (for example, the superficial implementation of such measures by the consumers or the ingenuity of the perpetrators). In such situations, the infringement of the law must be investigated, to establish the identity of the perpetrator and the exact nature of the crime which has been committed.

The investigation of crimes committed using IoT is performed by IoT Forensics. Usually, IoT Forensics is used to respond to threats like virus attacks, mass surveillance, Denial of Service (DoS) attacks, and disruption of IoT networks [23].

It is important to mention that IoT Forensics can be used not only when a cybercrime has been committed. For example, it can be used in the investigation of a burglary, if the criminal activity of the burglar has been recorded by a video camera connected to the Internet. If the events are recorded by a video camera which has no Internet connection, the investigation is perform by “traditional” Digital Forensics.

The investigations which must be done in the IoT domain have some specific features, which differentiate them from other investigations, even from “classic” digital investigations. The necessity to apply certain methods results from the specificity of the IoT. Thus, even if IoT is depending on computer technology and on the Internet, it has some defining characteristics which bring some prominent changes in IoT Forensics, when compared to forensics applied in other technological domains.

IoT Forensics is a branch of Digital Forensics. IoT Forensics refers to the activities aimed at identifying, extracting, and analysing digital information from devices that are a part of the IoT, which means that the devices must be connected to the Internet or to another network. By comparison, Digital Forensics encompasses the finding and examination of materials found in all devices which can store digital data. The “traditional” Digital Forensics retrieves information by investigating computers, servers, gateways, and smartphones in reference to the data which they can store by themselves, independent from a network connection. IoT Forensics can search for information by analysing devices which are connected to Internet or another network, hence included in the IoT (medical devices, public monitoring devices, traffic lights, smart cars, smart home appliances etc.). IoT Forensics also differs from Digital Forensics in what regards the type of evidence which is examined. IoT Forensics analyses data available in any vendor-specific format, while Digital Forensics analyses data mostly available in electronic documents or standard file formats [23], [24].

Summarizing, while Digital Forensics is any forensic investigation dealing with digital evidence, IoT Forensics is a specialized branch of Digital Forensics which investigates devices connected to the Internet or to another communication network.

9 The difficulties confronted by IoT Forensics

IoT Forensics faces many challenges, because of the specificity of the IoT, which brings new problems, which do not exist in the “classic” Digital Forensics. Most frequent issues are related to huge amount of data; complicated network topology; the specificity of the devices which form the IoT; the relation between the IoT and the cloud; lack of data standardization across vendors;
difficulties in decryption; data corruption; the need to respect privacy laws. In the following lines we will give a few details about each of these potential issues.

One of the main problems comes from the fact that IoT devices generate a huge amount of data. This brings difficulties in choosing the sources of evidence which are relevant for the case, and, in establishing the amount of data which will be further used in the investigation.

Another important issue in IoT Forensics comes from the complicated network topology existing in the IoT. Recognizing the network topology of the endpoints is a complex challenge in IoT Forensics.[25]

The physical accessibility of the devices can be a real problem for IoT forensic investigators. This comes from the fact that the devices connected on the same network might be in different places, and, even more, at great distances one from each other.[26]

The specificity of the devices which form the IoT adds other issues to IoT Forensics. IoT is formed by a high number of devices. Most of these devices do not carry out complicated tasks, as they are designed to perform simple tasks and exchange data between them. Many of the devices which are a part of the IoT have a small amount of storage.[26] This means that the information extracted from a single device usually does not offer much evidence, so it must be coordinated with other information.

The emphasis on the relation between the IoT and the cloud is another specific aspect. This means that it is not unusual to find the cloud as the base of the IoT network, or as a companion which performs the more complex tasks.[26] Such a situation requires a specific forensic approach.

A problem for IoT forensic investigators can be the lack of data standardization across vendors.[27]

Also, difficulties in decryption may cause important problems, especially because some data is heavily encrypted. If the encryption has been done with an atypical method or if the decryption token has been lost, it can be very hard to perform decryption.[28]

Data corruption is another issue, as data can be corrupted during transfer or as vendors store it over extended periods.[29]

IoT forensic investigations can be subject to restrictions when data protection laws and privacy laws are challenged. Some legislations allow storage companies to preserve data for a specific period and to make the data available to those who meet the legal requirements.[30]

Of course, labelling such elements as difficulties may be caused by the fact that IoT is a relatively new domain, and forensic investigators have not yet found proper solutions for all the problems raised by the IoT. In other words, the present-day difficulties may be caused by the fact that “classic” forensic tools and methodologies are not suitable for the challenges raised by IoT. However, IoT forensic experts have developed various automated methods to simplify the investigation and make it more efficient. This leads to “clean” data that can be extremely useful for solving a judicial case. Furthermore, we believe that, in the future, forensic investigators will do more and more adjustments to forensic tools, according to the specificity of IoT to improve the results of the investigation.

10 The basic notions regarding the IoT Forensics

In IoT Forensics it is essential to trace data because this can be used as evidence in a judicial case. Depending on the level upon which the examination takes place, an IoT forensic investigation may be composed of three types of examinations, corresponding to the structure where data is sought, namely the device, the network, or the cloud. This means that, basically, IoT Forensics implies a combination of three fields: IoT Device Level Forensics, Network Forensics, and Cloud Forensics.[31]

IoT Device Level Forensics refers to collecting evidence directly from the device. This process is often hard to accomplish, because of the wide variety of hardware and functionalities,
and because some devices store information only for a short period of time. Also, the data traces which can be found on devices may be corrupted [32].

Network Forensics is founded on the ability of networks used to transfer data to keep data traces for a period. Network Forensics tries to identify and extract information from network log, devices traffic traces and communication patterns. The process is not always prone to success, as data traces in networks are fragile and volatile. Also, difficulties may arise from the fact that networks use varied encryption methods, so investigators must use the appropriate network protocol [33].

Cloud Forensics is very important for IoT Forensics because most information collected by devices is stored in cloud. This is because the memory of the devices is usually limited. The result is that the cloud contains a massive amount of data. Cloud service vendors can provide data to those who have a legal right to ask the permission to collect evidence [31].

11 How the IoT Forensics works

Both IoT and IoT Forensics rely on sensors, which are installed in various smart devices (for example, a smart washing machine or a fitness tracker bracelet). These sensors collect data and, usually, the device transfers the data to the cloud. Here, the information is examined, stored, or prepared for other purposes. Because of the way that IoT works, IoT Forensics overlaps with Cloud Forensics, as the data has been transferred from the IoT devices to the cloud. As data travels through various networks and implies multiple sources, all these specific aspects lead to differences regarding the methods which are used to localize important digital evidence. Generally, any Digital forensic investigation must include provisions for multiple data formats and for multiple standards.

IoT forensic investigators usually must follow a list of six standard steps. This procedure is necessary, to maximize the results obtained through an investigation. These steps are Evidence Identification, Evidence Collection, Evidence Preservation, Evidence Analysis, Attack and Deficit attribution, Evidence Presentation [21].

Evidence Identification, the initial stage of the IoT forensic investigation, is very important and must be done with extreme accuracy, because the success of the whole investigation is rooted in it. This first step can be challenging, because many of the devices which form the IoT are small (for example, a medical bracelet), as they must not create difficulties for people wearing them [21]. As we have already said, most of the data collected by IoT devices is usually sent to cloud servers, because of the very limited memory of the device itself. This adds new challenges for the forensic investigation, because sometimes it is extremely hard to determine where the data is located, as it is distributed among many servers in multiple data centres [31].

Evidence Collection often raises difficulties, as, in most cases, it involves cloud evidence collection, and cloud data can often be located under different jurisdictions. This means that an IoT forensic investigation often involves multi-jurisdiction problems. As regards the device itself, once the IoT device has been identified, evidence should be extracted from its physical memory. As the cloud almost substitutes the storage (ROM) of the IoT devices, most of the physical information can, still, be retrieved from the volatile memory (like RAM). To collect evidence from the physical memory, “traditional” Digital Forensics recommends investigators to turn off the devices, to prevent the data alteration. But, in IoT Forensics, the practice is to try to collect evidence without shutting down the device. In other words, in IoT Forensics it is preferred to collect information through live data acquisition, although this cannot always be performed, because of the limited energy of the device [24], [34]. Specialists have developed some useful tools that can be used by IoT forensic investigators to identify and collect evidence, but these tools usually require proactive process (which means installing the software before the cybercrime is committed) [31].
Evidence Preservation means keeping the information that has been gathered and guaranteeing its integrity during the full process. The specificity of the IoT makes the “traditional” methods of preservation used in Digital Forensics inappropriate for IoT Forensics. Usually, blockchain solutions are being used, with the main aim to protect the evidence from cyberattacks [35].

Evidence Analysis is closely linked to Attack and Deficit attribution. These stages refer to the thorough analysis and corroboration of all the evidence, to reach a conclusion, including to identify the perpetrator. In “classic” Digital Forensics, completing these stages can be easier, because, usually, there is a limited number of suspects, as the evidence is commonly extracted from personal devices (meaning that the owner or the user of the device is easier to establish). This is not the case in IoT Forensics. Here, the huge amount of data makes it very hard to perform an end-to-end analysis. Usually, IoT devices do not store any metadata, including temporal information (such as creation or modification times), and this increases the difficulty to verify the source. Even more, as we have already said, in IoT Forensics evidence is in most cases collected from the cloud, meaning that it can be located in physical servers accessed by several users simultaneously [21], [24]. However, some solutions have been found. For example, in order to analyse the big amount of data collected from IoT, Artificial Intelligence and Machine Learning are being used [36].

Evidence Presentation is the last stage of any forensic investigation. Unlike in “traditional” Digital Forensics, in IoT Forensics this step may be difficult. This is because the evidence collected through IoT Forensics has usually an abstract form, which is hard to understand for those who are not specialists in IoT (no matter if they are judges or jurors). Giving such situation, the IoT forensic investigator must present the information in a form which is easy to understand for people who are not IoT experts. By contrary, if the evidence is kept in its abstract form, it may not be considered in court [24].

It is important to highlight the fact that IoT forensic investigations must respect all standard guidelines, meaning all legislation which refers to the forensic procedure, as a condition for the admissibility on the court of the evidence which has been collected [32].

12 Conclusions

The Internet of Things (IoT) offers many benefits to the human society, enabling people to have a life greatly improved with the help of high technologies. This is something that, for decades, only writers of science fiction literature have brought into discussion, making people dream of the wonders of such a world. Now, this kind of world has become reality. Even more, it evolves from day to day, because technologies develop very fast, creating new ways to enhance life quality using devices connected to the Internet or to another type of communication network. But IoT does not apply only to individuals. It applies at a bigger scale, in a process which seems prone to creating a high-tech human society. Many cities have already become smart, as they use IoT to solve problems related to traffic and pollution. Even agriculture is becoming smart, with IoT being used to maximize the yield and to minimize the loss. IoT is also used in various industries, helping disadvantaged regions to make significant progress towards a better economy. It looks like there are no limits for the benefits which the IoT can bring for humans, and only time will reveal the true potential of this seemingly fantastic technological domain.

There is only one problem which overshadows the promise of an extraordinary future, based on IoT. This problem is deeply rooted in the human nature and refers to the anti-social acts committed by some people. Along the history, almost every major human achievement has been accompanied by the activity of those who wanted to take undeserved benefits, using that achievement. It is, also, the case with the IoT. The great benefits which IoT bring come with a price, namely the fact that many people are willing to use IoT for malicious purposes, for their own mean interests. These people exploit the specific features of the IoT, which depends on data.
sharing between various devices. The same characteristics which make the IoT so easy to use by *bona fide* costumers make it an easy target for cyberattacks.

To restore the social order that has been broken by the cyberattack, special methods must be used, with the purpose of identifying the perpetrator and finding out the type of crime and the amount of the damage. These special methods are the object of IoT Forensics, which is a specialized branch of Digital Forensics. IoT Forensics works as a combination of three types of forensic methodologies, depending on the level upon it performs the investigation, namely the device, the network, and the cloud. Because it is hard to find evidence on devices and networks, most evidence is collected from the cloud. IoT Forensics faces many challenges due to various factors like: the limited memory of the devices, which usually share data in the cloud; the huge amount of data found in the cloud, which requires special methods of analysis; the multi-jurisdiction issues which may appear, as cloud data can often be located under different jurisdictions.

Despite all difficulties, IoT forensic investigators have, so far, found efficient methods, to solve judicial cases related to IoT cybercrime. Also, it is important to mention that IoT Forensics is a dynamic field, where experts are permanently seeking for new solutions, better adapted to the uniqueness of the IoT domain. The efforts of the IoT forensic investigators are, undoubtedly, worthy, because their scope is to help people to have faith in the benefits which IoT can bring. And, along with trust in the IoT, people may also gain trust in the fact that the future can, indeed, be a technological utopia.

**References**


