Internet of things security: A top-down survey

Djamel Eddine Kouicem, Abdelmadjid Bouabdallah, Hicham Lakhlef

Internet of Things Security: a top-down survey

Djamel Eddine Kouicem[a], Abdelmadjid Bouabdallah[a], Hicham Lakhlef[a]

[a]*Sorbonne Universités, Université de Technologie de Compiègne*
CNRS, HEUDIASYC UMR 7253
CS 60319; 60203 Compiègne Cedex, France

Abstract

Internet of Things (IoT) is one of the promising technologies that has attracted a lot of attention in both industrial and academic fields these years. It aims to integrate seamlessly both physical and digital worlds in one single ecosystem that makes up a new intelligent era of Internet. This technology offers a huge business value for organizations and provides opportunities for many existing applications such as energy, healthcare and other sectors. However, as new emergent technology, IoT suffers from several security issues which are most challenging than those from other fields regarding its complex environment and resources-constrained IoT devices. A lot of researches have been initiated in order to provide efficient security solutions in IoT, particularly to address resources constraints and scalability issues. Furthermore, some technologies related to networking and cryptocurrency fields such as Software Defined Networking (SDN) and Blockchain are revolutionizing the world of the Internet of Things thanks to their efficiency and scalability. In this paper, we provide a comprehensive top down survey of the most recent proposed security and privacy solutions in IoT. We discuss particularly the benefits that new approaches such as blockchain and Software Defined Networking can bring to the security and the privacy in IoT in terms of flexibility and scalability. Finally, we give a general classification of existing solutions and comparison based on important parameters.

Keywords: Internet of Things; Security; Privacy; Cryptography; Blockchain; Software Defined Networking

1. Introduction

Nowadays, Internet of Things (IoT) is changing much about the world we live in, the way we drive, how we make decisions, and even how we get energy. Internet of things consists of sophisticated sensors, actuators and chips embedded in the physical things that around us by making them smarter than ever. These things are connected together and exchange huge data between them and with other digital components without any human intervention [3]. IoT contributes significantly to enhance our daily life throughout many applications come from different sectors such as smart cities, smart building, healthcare, smart grids, industrial manufacturing among others.

Currently, one of the issues that potentially threats Internet of Things' devices is the security and the privacy of exchanged/collected data that are often deeply linked to the life of users. Gartner [1] envisioned that, by 2017, more than 20% of organizations and businesses will deploy security solutions to protect their IoT devices. These considerations lead us to underline the importance of enforcing security mechanisms in IoT applications which play a pioneer role in mitigating IoT risks. Security problems in IoT are most challenging than the existing security problems in Internet of nowadays. Indeed, it is instructive to note that the things are highly resources-constrained in terms of computing capacity, memory and energy which make the existing security solutions absolutely not applicable. Moreover, the high number of connected objects, estimated by Cisco [46] to be about 50 billions of objects by 2020, arises scalability issues.

These last years, a lot of researches are leading to address the various security challenges closely related to IoT such as key management issues [114], confidentiality, integrity, privacy, policy enforcements [110, 113] among many other challenges. The main works in the literature tried to adapt the security solutions proposed for wireless sensor networks (WSNs) and Internet in the context of IoT. However, we must point out that IoT's challenges take a new dimension which is far from being easy to overcome with traditional solutions. In addition, we must emphasize that most security approaches rely to centralized architectures, making their applications in IoT much more complicated regarding the large number of objects. So, distributed approaches are required to deal with security issues in IoT. In this paper, we survey the different solutions according to two perspectives, namely the security approaches based on traditional cryptographic approaches and the other approaches based on new emerging technologies as SDN and Blockchain.

In the literature, there are some published surveys that cover different aspects of security in IoT. In [14, 74, 127, 137, 108, 66], authors underlined the security challenges and issues in IoT without discussing the various solutions proposed for these challenges. Moreover, Roman et al. [104] discussed the main benefits and also the important issues to be addressed in terms of security and privacy in decentralized architectures.

[1] https://www.intrinsic-id.com/intrinsic-id-guardtime-announce-alliance-iotblockchain/

Other surveys are oriented IoT domain applications. In [41, 36] provided an overview about security and privacy challenges in smart grids. Other applications are also discussed in other papers. We can cite Healthcare application in [4] and industrial IoT in [105]. Alaba et al. [5] investigated the main security vulnerabilities and attacks in IoT.

Other surveys dealt with IoT security issues and reviewed solutions according to each security service. In contrast, in [111], the authors investigated confidentiality, access control, trust management and privacy solutions in IoT. On the other hand, in [98] Ouaddah et al. reviewed access control solutions. In [94], Kim et al. gave a classification of key management solutions in IoT. In those surveys, the authors focused particularly on classical based cryptographic approaches without discussing the new relevant techniques which could potentially bring huge values in terms of security and privacy.

Intrusion detection in IoT is another important research field which has received a high interest of researchers. Some surveys [25, 89] have discussed intrusion detection systems (IDS) in wireless sensor networks and Internet of Things and have provided analysis and comparison of the main existing IDSs.

The main common line between the existing surveys is that most of them focus on cryptographic solutions which belong to centralized approaches. However, recently, many emergent technologies (ex. blockchains, SDN) are being adopted by industrials (ex. IBM's IoT based blockchain solution, named ADEPT) as promising solutions to fix security and privacy issues in IoT that have not been addressed in all existing papers. In this survey, we take a different direction by enumerating the different security approaches, including recent ones and classify them into two main categories: classical approaches and new emerging techniques. Furthermore, we provide a top down review that offers a holistic view of the security in Internet of Things. This review encompasses in three steps the different aspects of security in IoT by starting from generic to specific aspects. We start by enumerating the different challenges related to the various IoT applications. Subsequently, we discuss in more details the several solutions of IoT security recently published in the literature. Finally, we finish our survey with a synthetic comparison and discussion about the most relevant solutions for each IoT application with respect to the several security challenges. By positioning with respect to the aforementioned surveys, the table 1 shows clearly that the contribution of this paper includes, in a comprehensive way, the most relevant aspects such as lightweight cryptographic approaches, blockchain, the context awareness and the coupling security-safety in IoT. All these aspects constitute the main recent research pieces in the field of Internet of Things security and privacy.

The main contributions of this survey are threefold:

- Present the different security challenges and requirements for the main IoT applications, i.e a top down approach.
- Survey the literature solutions according to two main points of view (classical and new emerging approaches).
- Finally, provide a comparison of the enumerated approaches based to some parameters; and investigate the possibility of applying such approach on a given IoT application.

	[105]	[89]	[111]	[94]	[5]	[14]
Smart grids	Yes	No	No	No	Yes	No
Smart cities	No	Yes	No	No	Yes	No
Healthcare	No	No	No	No	Yes	No
Manufacturing	No	Yes	No	No	Yes	No
Transport	Yes	No	No	Yes	Yes	
Confidentiality	Yes	No	Yes	Yes	Yes	Yes
Privacy	No	Yes	Yes	Yes	No	Yes
Availability	Yes	No	No	No	Yes	Yes
Blockchain	No	No	No	No	No	No
SDN	No	No	No	No	Yes	No
Context-awareness	Yes	Yes	Yes	No	No	No
Safety-Security	Yes	Yes	No	No	No	No

Table 1
Recent surveys in IoT security

The rest of the paper is organized as follows. Section 2 gives a background about the main security services and the main known techniques to fulfill each service. We discuss and summarize, in section 3, the main security challenges and requirements of some well known IoT applications. In section 4, we provide our classification of security solutions. In section 5, we describe in details the main classical approaches proposed in literature, we classify those approaches according to security services. New emerging approaches based on blockchain and Software Defined Networking technologies are described in section 6. We discuss in section 7, the importance of context awareness to mitigate security in IoT. Section 8 gives details about design approaches of security and safety in Cyber-Physical based IoT systems. Section 9 provides a comparison of the proposed security solutions and their applications in the different IoT sectors. Section 10 concludes the paper.

2. Background on security services

Security consists of all the techniques that aim to preserve, restore and guarantee the protection of information in computer systems from malicious attacks. Daily news puts security at the top of concerns: leakage of personal data and economic espionage, infection of sensitive computer systems, identity theft and fears about card payments are just few examples of threats. The security of computer networks and information systems in general, consists to provide the following services [96]:

- **Confidentiality**: It ensures that information is made unintelligible to unauthorized individuals, entities, and processes.
- **Integrity**: It ensures that data has not been modified by a third party (accidentally or intentionally).
- **Authentication**: It verifies that the data source is the pretended identity.

Security services	Security mechanisms	Some examples
Confidentiality	message encryption / sign-encryption	symmetric cryptographic mechanisms (AES, CBC, etc); asymmetric mechanisms (RSA, DSA, IBE, ABE, etc).
Integrity	hash functions, message signature	hash functions (SHA-256,MD5, etc); Message Authentication Codes (HMAC)
Authentication	chain of hash, Message Authentication Code	HMAC, CBC-MAC, ECDSA
Non-repudiation	message signature	ECDSA, HMAC
Availability	pseudo-random frequency hopping, Access control, Intrusion prevention systems, firewalls	Signature-Based Intrusion Detection, Statistical anomaly-based intrusion detection
Privacy	pseudonymity, unlinkability, k-anonymity, Zero Knowledge Proof (ZKP)	EPID, DAA, Pedersen Commitment

Table 2
Security services and mechanisms

- **Non-repudiation**: It ensures that the sender of the message can not deny having sent the message in the future.
- **Availability**: It ensures that the services of the system should be available for legitimate users.
- **Privacy**: It ensures that users' identities should not be identifiable nor traceable from their behaviors and their performed actions in the system.

Several cryptographic mechanisms have been put in place to deal with the different security threats and ensure the security services mentioned above. We provide in table 2 some of those mechanisms.

3. IoT Applications: security requirements and challenges

Internet of Things enables to improve several applications in various fields, such as, healthcare, smarts grids, smart cities, smart homes as well as other industrial applications. However, introducing constrained IoT devices and IoT technologies in such sensitive applications leads to new security and privacy challenges. In this section, we illustrate some important IoT applications and highlight the security requirements and challenges of each application.

3.1. Smart Grids

Electrical energy is a treasure which has a very high industrial value, and plays an important role in economic development. Nowadays, we use very modern IT technologies to optimize electricity production by taking into account user demands throughout the electricity distribution line. The smart grid is the technology behind this distribution line. It consists of an integrated network, called also the advanced metering infrastructure (AMI) installed between the electricity production centers and the end customers, whose important role is to coordinate the electricity production with respect to the consumption of end customers. Smart grids represent one of the most attractive areas in IoT. The main goal is to improve the quality of experience of final customers and optimize the electricity production. To better understand in more details how IoT can improve the electricity production in smart grids, the reader is referred to [78, 36].

3.1.1. Security requirements

Several works [36, 68] underlined security requirements that must be considered in smart grids. In what follows, we highlight the most important requirements in terms of security and privacy:

- **Availability**: The network infrastructure, smart meters as well as the control center that handles optimization queries and control commands should be available continuously. Moreover, unauthorized users should not deny authorized users to handle queries.
- **Confidentiality**: The exchanged data and queries between smart meters and control systems are sensitive and must not be disclosed by third unauthorized entities.
- **Integrity**: Regarding the type of data exchanged between smart meters and control systems, they are very useful for decision making to optimize energy transmission. Integrity of this data is very important for better decision making. We should also deal with injection attacks that try to inject in the AMI infrastructure false measures that could disturb decisions making.
- **Non-repudiation**: Any entity in the system among the utility servers and the smart meters does not deny that it has not received some data or control commands subsequently.
- **Privacy**: exchanged information in AMI infrastructure contains fine-grained pieces of data about the electricity consumption in houses and buildings. This private data reveals information about customers' activities in houses and companies. It's mandatory to protect this data and make it untraceable.

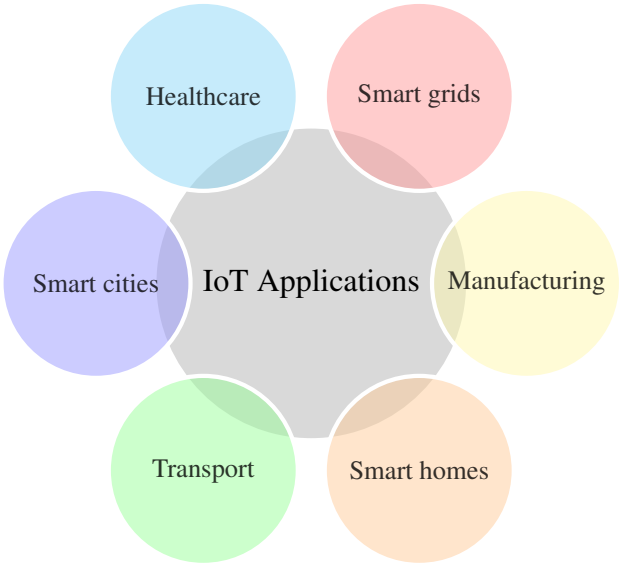

Fig. 1. Internet of Things' applications.

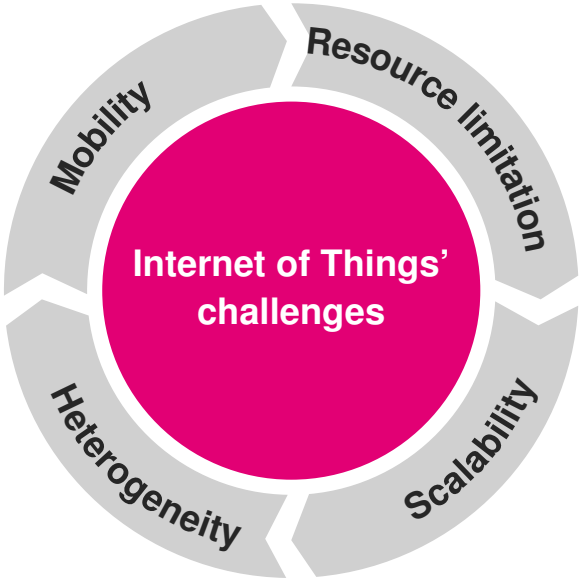

Fig. 2. Internet of Things' challenges.

3.1.2. Security challenges

Smart grids should resist against some security challenges. In the following, we present the important ones:

- **Heterogeneity** of communication standards and information system technologies in smart grids.
- **Scalability issues**: as the population and their electrical energy consumption grow faster these years, the number of smart meters and control centers grow explosively. Therefore, security solutions face serious scalability problems.
- **Vulnerabilities related to information system technology**: as smart grids are open, we can imagine any kind of attacks that could threat harmfully the availability of the AMI network. Integrity, confidentiality and privacy of data, IP spoofing, injection, DoS/DDos attacks are just examples of attacks among others.
- **Data sensitivity and privacy**: Exchanged information between smart meters and the control center includes sensitive data about customers like electricity consumption, real-time usage of smart meters for each customer. This information must not be leaked by neighbors while keeping it exploitable by control center.

3.2. Healthcare

Smart healthcare plays a significant role in healthcare applications through embedding sensors and actuators in patients' bodies for monitoring and tracking purposes. The IoT is used in healthcare in order to monitor physiological statuses of patients. The embedded sensors have the ability to collect information directly from the body area of the patient and transmit it to the physician. This technology has the potential to completely detach the patient from the centralized system which is the hospital while maintaining continuous contact with the physician. Currently, Healthcare based IoT applications represent one of the promising technologies that impact hugely the society which is mainly due to the aging of the population. Indeed, in France, the percentage of people over the age of 60 reached about 24% of the population in 2015 and will rise to 32% by 2060 [2]. Furthermore, the budget reserved for healthcare applications reached about 12% of the GDP (Gross domestic product) [3]. In this context of population aging and the cost related to the treatment, a great interest emerges to adopt new IoT based technologies to monitor the patients in real time.

3.2.1. Security requirements

Based on preliminary studies [4], we summarize the privacy and security requirements in healthcare applications as follows:

- **Authentication**: The access to PHRs (Personal Health Record) related to each patient must be protected against non authorized individuals, only physicians and nurses are able to access these records.
- **Confidentiality and Integrity**: It's mandatory to secure communications between patients and hospitals by ensure confidentiality and integrity of exchanged data.
- **Privacy concerns**: Patients should know, in real time, who owns and manipulates their PHRs. In addition, it's necessary to hide IoT devices' locations, patients' identities, etc.

3.2.2. Security challenges

Note that there are a lot of security and privacy challenges issuing from healthcare applications that must be overcome. We highlight, hereafter, the most important challenges:

[2] https://www.insee.fr/en/statistiques/1281166
[3] https://www.insee.fr/fr/statistiques/1906695?sommaire=1906743

- **Resources limitations**: most of embedded sensors and wearable have limited resources in terms of computation, memory and battery. Since the most of cryptographic solutions are computationally expensive, adapting them to ensure a high level of security while minimizing energy consumption is a hard challenge.
- **Mobility**: sensors and actuators are embedded in human bodies which in general are mobile. Taking in consideration mobility in security solutions is a serious challenge.
- **Heterogeneity**: the communication between sensor nodes and hospital servers or CPU units in general are done over Internet where networks, protocols and communication mediums are heterogeneous and have different security configurations. Moreover, sensor devices measure physiological data (heartbeat, body temperature, etc) which are heterogeneous in terms of units of measurements and delivery frequencies. Developing an adaptive security solution that works in heterogeneous environments is extremely challenging.

3.3. Transportation systems

Intelligent transportation systems (ITS) represent the next generation of transportation that aims to link people, roads and intelligent vehicles thanks to the development of embedded systems and communication technologies. By connecting and distributing intelligent processors inside vehicles and also through transportation infrastructure, we can make the transportation safer, greener and more convenient. ITS employs four main components, namely: vehicle subsystem (consists of GPS, RFID reader, OBU, and communication), station subsystem (roadside equipment), ITS monitoring center and security subsystem [76]. Connected vehicles are becoming more important with the aim to make driving more reliable, enjoyable and efficient [50]. Actually, we have three types of communications in vehicular networks: V2V (Vehicle to Vehicle), V2I (Vehicle to Infrastructure) and V2P (Vehicle to Pedestrian) [76]. However, recently, a new type of communication has emerged, called V2G (Vehicle to Grid), whose main goal is to ensure electrical Vehicles charging based on energy of smart grid electricity distribution [78].

3.3.1. Security requirements

There are some security concerns need to be considered in order to secure different types of communications in vehicular networks.

- **Authentication**: It's mandatory to authenticate senders of messages.
- **privacy**: Privacy of drivers must be protected against unauthorized observers. Their identities must not be revealed to neighbors.
- **Non-repudiation**: Drivers causing accidents should be reliably identified.
- **Availability**: Vehicular Networks should be available and must persist to jamming attacks [122] aiming to disturb communications between vehicles.

All of the above requirements are more or less well studied in literature. However, new similar and additional security issues in V2G (Vehicle to Grid) should be studied furthermore, for example:

- Secure transactions between vehicles and smart grid network providers.
- Privacy concerns are more interesting in V2G communications. Indeed, we need to hide sensitive information such as: location, charging time, the amount of battery, etc. from intruders while maintaining this information accessible from authorized entities for optimization and charging coordination purposes.

3.3.2. Security challenges

There are many challenges to which intelligent vehicles and intelligent transportation systems face and make their security more complicated to achieve:

- **Diversity of attacks' sources**: vehicular networks are exposed to all kinds of attacks (inside and outside) which harm the safety and the privacy of drivers. Exchanged information must be securely delivered and protected from any kind of attacks in order to avoid damages and accidents [87].
- **High mobility**: intelligent vehicles evolve in highly dynamic environments, where changes in the network topology are made frequently. This makes the deployment of security solutions highly challenging.
- **Heterogeneity**: The diversity of the entities involved in the transportation system [87]. Attacks could come from any of those entities or from a set of entities conducting a Distributed Denial of Service (DDoS) attacks.

3.4. Smart cities

Smart cities consist of one of the most important applications of IoT. Although, there is no formal definition of "smart city", it consists of a new emerging paradigm that aims to enhance the usage of public resources, increase the quality of service to citizens [135]. In this context, sensors are deployed all over roads, buildings, smart cars, etc. to better manage traffic, adapt to the weather, lighting follows the position of the sun, domestic incidents can be avoided with alarms, etc.

3.4.1. Security requirements

Smart cities claim a lot of security requirements:

- **Confidentiality** of information and access control of sensitive data.
- **Authentication** of users and information's origins.

Challenges \ Applications	Smart grids	EHealth	Transportation systems	Smart cities	Manufacturing
Resources constraints	+	+++	-	++	+
Mobility	+	++	+++	+++	-
Heterogeneity	++	++	++	+++	+
Scalability	+++	++	+++	+++	++
QoS constraints	++	++	+++	+++	+++
Data management	++	+	++	+++	++
Lack of standardization	++	++	++	++	+++
Amount of attacks	+	+	+++	+++	+++
Safety	++	++	+++	++	+++

Table 3
Main Security challenges

- **Integrity of data** is also very important as these pieces of data are sensitive and participate in decision making and enhance the daily life of citizens in the smart cities.
- **Availability of information** for users and decision-makers.

3.4.2. Security challenges

Several security and privacy concerns are necessary to be addressed in the smart cities. In what follows, we present the most important challenges:

- **Very high level of heterogeneity**: in smart cities, heterogeneous smart devices (in terms of capabilities, behaviors, goals, etc.) are deployed anywhere in cities and are gathered together in one single ecosystem. In addition, there is no communication standard for all the components that behave differently, which are also dedicated for different applications.
- **Scalability**: It is another serious challenge regarding the number of smart devices that continues to grow daily.
- **Data management issues**: several challenges arise about the management of the huge amount of data generated by smart devices in the smart cities. Actually, many questions arise: how to locate data, control access to this data and preserve its integrity and privacy.

3.5. Manufacturing

Nowadays, IoT plays an important role in the industry. It is considered as a promising solution to automate the process of manufacturing and the control of the production chain. Industrial Internet of Things (IIoT) uses new technologies such as Machine-to-Machine (M2M) communication, Wireless Sensor Networks (WSN), automation technologies as well as Big Data to create an intelligent industrial ecosystem [105]. The main aim of IIoT is to provide better productivity, efficiency, reliability and better control of final products.

3.5.1. Security requirements

IIoT systems claim the following important security requirements:

- **Availability of the system**: It's very fundamental that the manufacturing system continues to operate even under critical situations. This includes particularly the deployment of DoS countermeasures to maintain the availability of the system. Cyber-Physical systems subjected to real-time constraints introduce new challenges. To launch DoS attacks, the adversary can: 1) jam communication channel, 2) compromise sensors and prevent them to send measurement, 3) disrupt routing protocols, etc.
- **Integrity** : Any industrial system needs a reliable information to prevent any failure or physical damage. Thus, we need to preserve the integrity of the exchanged information between IoT devices behind the industrial system. Integrity issues might also cause safety problems in Cyber-Physical Systems when Industrial IoT components receive false data and believe it to be true.
- **Confidentiality**: The manufacturing process is very secret and sensitive against espionage attacks. Therefore, we must protect data, code, system configurations by means of encryption mechanisms.
- **Authentication**: In manufacturing systems, some production tasks are outsourced to third parties. Therefore, it's mandatory that these third parties must be authenticated and prove its trustworthiness.

3.5.2. Security Challenges

In IIoT, there are serious security challenges that need to be addressed:

- **Cyber-Physical attacks**: Manufacturing system is one of the most targeted systems by attackers [105]. Trojans, viruses, DoS/DDos attacks and software compromises are just few examples among others.
- **Scalability issues**: As manufacturing Cyber-Physical Systems grow continuously, security solutions should deal with this expansion.

- **Lack of standardization**: In practice, there is no existing standard protocol that is adopted in all SCADA based IoT systems. Indeed, there are about 150 to 200 open standards [88].
- **Resources limitation**: IoT devices and actuators used in manufacturing field which are in general employed in practical architectures that claim low cost and present constraints in terms of computation and power.
- **Safety challenges**: Manufacturing systems in general and SCADA systems in particular are vulnerable to several type of attacks, namely: misuse of resources, user compromise, root compromise, virus, social engineering, torjan, worm, denial of services, etc [26]. These attacks impact hugely SCADA systems by disclosure, disrupt, distort and destruct control messages which might cause big damages that harm the safety of the hole system. In 2010, a group of unknown attackers created complex worm called Stuxnet [4] which is one of the most known attacks that aimed at disrupting control messages in SCADA systems. It targeted only controllers from one specific manufacturer (Siemens). This worm caused a lot of safety damages in SCADA based control systems. Experiences demonstrated the importance of enforcing security and safety mechanisms in SCADA systems in particular and Industrial Internet of Things in general. Risk assessments design tools that consider both of safety and security are necessary in order to anticipate some countermeasures against malicious attacks in the early stages of industrial system design. In section 8, we discuss in more details this important challenge of safety in manufacturing systems which is related to security attacks. We discuss also the several solutions to overcome this challenge.

3.6. Discussion

In the light of the challenges and the security requirements of the main IoT applications presented above, we provide in table 3 a summary of those requirements by highlighting the main aspects inherent to each IoT application.

In the high level picture, the security in IoT applications is considered as a hard issue to solve and it faces a lot of challenges. Basically, we highlight resources constraints, heterogeneity and scalability challenges which are more likely common to several applications. Indeed, most of applications operate in highly distributed environments with the use of heterogeneous smart objects, sensors and actuators that are limited in terms of power and computation resources [94, 111]. These three challenges make the security very hard to solve with current approaches. Indeed, these later are based on greedy cryptographic tools operating on centralized environments (the need to central trust authorities to manage cryptographic keys for objects) and thus they are not suitable for IoT applications which are distributed [94]. Moreover, the huge amount of objects that are implicated makes that the security issues even more complicated. At this stage, we might think about the application of new emerging techniques such as blockchain and SDN to meet more efficiently these challenges. We discuss in the sections 6.2 and 6.2, the main benefits of these techniques.

Other challenges are more likely inherent to some specific applications such as the mobility challenge in transportation systems and the lack of standardization in manufacturing systems and smart cities applications [88]. These challenges should be investigated separately and carefully in each application in order to meet the requirements of each application. We can think about the high mobility of connected cars that could make the trust management problem a very hard task to achieve compared to other applications where the mobility is low [55, 131].

We note also that some IoT applications present safety challenges that must be addressed jointly with the security regarding the complex relations between the two aspects [115]. Manufacturing system is an example of these applications. Indeed, security attacks in control systems could impact the configuration of this later and thus will evolve safety problems [115, 22]. We will discuss in more details these challenges related to safety and security in manufacturing based IoT systems in section 8.

4. Taxonomy of security solutions in IoT

Security subject is one of the hot research problems in IoT and has attracted a lot of researchers not only from academic and industry but also from standardization organizations. To date, there have been a lot of proposals aiming to address the security problems in IoT. In this section, we propose a classification of these solutions from an architectural point of view and we illustrate in figure 3, our classification of security solutions in Internet of Things. We distinguish in the light of this classification two main categories of approaches:

1. **Classical approaches**: this category of solutions groups the cryptographic based techniques that were especially designed for IoT communications or have been adapted from wireless sensor networks or M2M communications. In section 5, we present only the most significant solutions and we provide the main limitations of each proposal. We note that in this survey, we focus basically on solutions that ensure: confidentiality, privacy and availability services. It is worth mentioning that most of these solutions operate in centralized environments where we have central trusted entities ensuring the proper functioning of the security services. The cryptographic tools employed to ensure the security services are whether symmetric or asymmetric techniques that we will discuss by pointing out their main advantages and limitations in the context of IoT for each security service.
2. **New emerging security solutions**: This category groups security solutions that are based on new techniques other than cryptographic tools. They are more convenient to meet the scalability issues compared to cryptographic approaches. In general, the solutions belonging to this category are decentralized. In section 6, we focus on two emerging technologies :

[4] http://large.stanford.edu/courses/2015/ph241/holloway1/

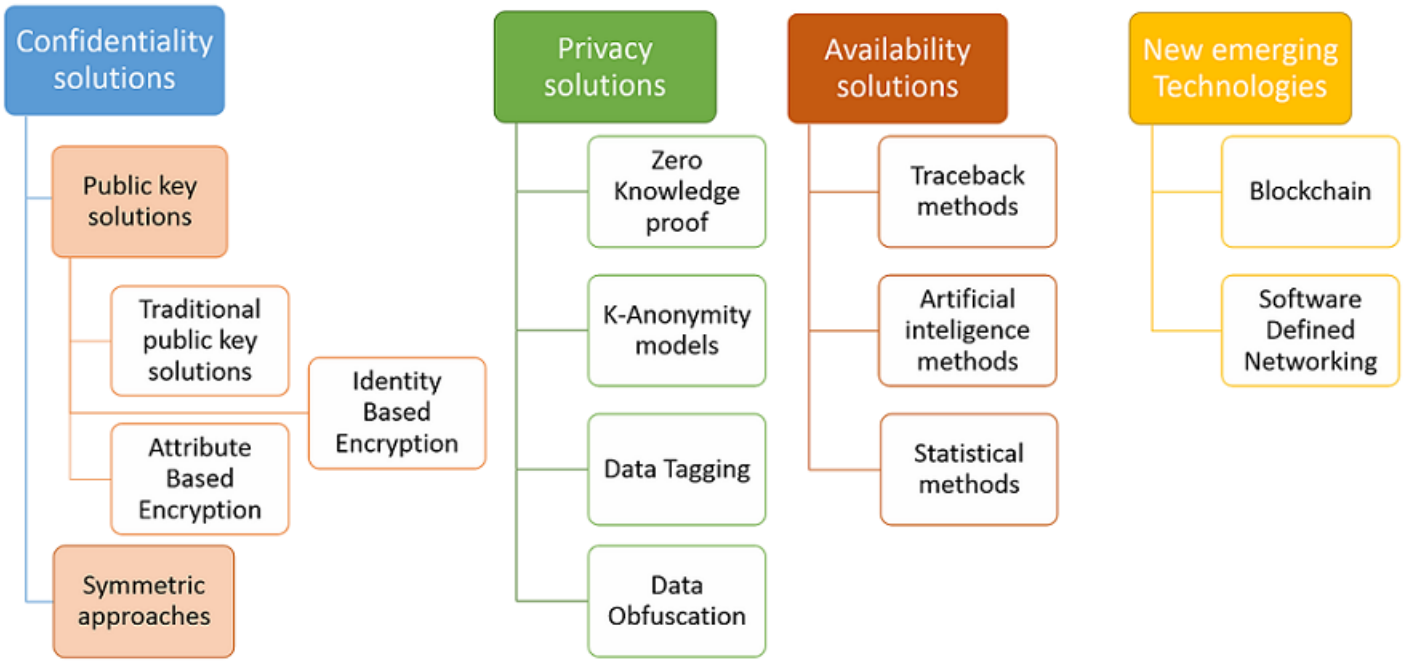

Fig. 3. IoT security solutions

(a) Software Defined Networking (SDN), which is a new network paradigm that is revolutionizing the world of networking this last years. Its aim is to provide an environment to develop more flexible network solutions and make the network resources more easy to manage using centralized SDN controller. Many SDN based security solutions for IoT have been proposed in the literature. We will discuss in more details these solutions in section 6.1.

(b) Blockchain technology, which is the technology behind the cryptocurrency tools such as bitcoin, aims to make the transactions between entities in a distributed manner (peer to peer architecture without referring to any central trusted server. Moreover, this solution does not require that entities trust each other. In this technology, it is piratically impossible to deny performed transactions once they are validated. Beside its application on the cryptocurrency domain, these last years, a lot of researchers have started to put the light on this technology in order to address security solutions in IoT such as data privacy, access control, etc. We present an analysis of these solutions in section 6.1.

We present mainly in section 6 the benefits of SDN and blockchain in terms of security, their key advantages, the issues that these technologies can solve and classical approaches can't and also their limitations.

Even though the solutions presented in sections 5 and 6 address most of the important challenges such as scalability, resource limitations, they are still not convenient enough in dynamic IoT environments such as vehicular networks where the context evolves frequently. Often, the context groups many pieces of information about the IoT objects locations, their battery levels, the number of their surrounding objects, etc. These pieces of information might be relevant to enhance the security and thus they can be applied to design more flexible and context-aware security solutions without referring to cryptographic approaches. From our perspective, context-awareness solutions could be shown as complementary techniques with respect to cryptographic solutions. For example, considering a heavy cryptographic algorithm to authenticate one IoT device A. In some situations, it is interesting sometimes to:

- Not perform the adopted cryptographic algorithm to authenticate A because it does not have sufficient energy to perform the heavy cryptographic operations and thus saves its battery while it is situated in a safe area.
- Consider other information related to device A to identify it without relying to cryptographic mechanisms. This information could be the location of A, the date of its last authentication, the owner of A, etc.

We will discuss in section 7 furthermore context-awareness solutions, how they can be applied to enhance the security in IoT and their potential benefits.

5. Classical IoT security approaches

In this section, we review and discuss the main proposed solutions which are based on cryptographic approaches to address the main security services. Considering the traditional approaches, we focus on: confidentiality, availability and privacy services.

5.1. Confidentiality solutions

In Internet of Things, we need to protect data exchanged between objects from attackers by means of encryption mechanisms. Hence, we should ensure that only legitimate users are able to disclose encrypted data. For this goal, cryptographic solutions exist to ensure data confidentiality, however, in most cases, these solutions are inefficient or even inapplicable in IoT devices with high resource constraints because they are based on algorithms that are very greedy in terms of storage and computation. To get an idea about the energy consumption and the effeciency of the different cryptographic algorithms, the reader is invited to read the paper of Malina et al. [85] where intensive analysis was investigated to compare the different cryptographic primitives widely used in security and privacy. Considering the power limitation of smart objects, a lot of cryptographic solutions have been proposed to deal with resources constraint's issues. Basically, these solutions belong into two main classes, namely symmetric and asymmetric cryptographic solutions.

5.1.1. Symmetric key solutions

In Symmetric key schemes, each entity in the system should share cryptographic keys with all other entities in the system. The main advantages of symmetric based cryptographic solutions are their efficiency (they are less-computational) and easy to implement in hardware platforms. AES (Advanced Encryption Standard), RC4 and 3DES are just few examples widely used in practice. Although their efficiencies, symmetric key based security solutions suffer from scalability and key management issues. Indeed, this latter emerges as serious problem in Internet of Things where there are a lot of devices that exchange sensitive data in dynamic environments. In Symmetric key based solutions, each device must keep secret keys with all the devices evolving in the IoT system in order to exchange sensitive data. Basically, we can distinguish between two key distribution approaches [53], namely : 1) Probabilistic key distribution and 2) Deterministic key distribution.

In deterministic approaches, each entity must be able to establish a secure link with all other entities to form a full secure connectivity coverage. Therefore the number of shared keys in the system increases quadratically according to the number of entities (for n entities, we need $n(n-1)/2$ keys). Depending on the presence or not of a trust third party during key bootstrapping, we distinguish two sub-categories [53], namely : 1) offline key distribution approach where nodes can share session keys with a distributed way without the intervention of any central entity; and 2) Server-assisted key distribution where we dispose of a central server that is charged of expensive cryptographic computations and attributes session keys to IoT devices. In contrast, Leap scheme [138] uses a kind of temporary key which is kept in sensor nodes to generate session keys and is removed from the memory when the key agreement is done. For security purposes, Leap requires that sensor devices must not be exposed to attacks during a predefined time after the deployment. In [30], the authors proposed a memory-efficient key management scheme that reduces the storage to only $(n-1)/2$ keys per node. The main idea consists to introduce new mechanisms based on a hash function to generate half of symmetric keys while storing the other half in sensors' memories.

In Probabilistic key distribution, it's not guaranteed that each node in the network shares a secure key with all other nodes, but the nodes share keys with their neighbors according to some probabilities in such way we must be able to form secure paths [5] between all entities in the network. With this approach, the scalability issues are solved, but the key management protocols become less resilient in case of nodes' comprises. In the literature, there are a lot of probabilistic key management schemes. The first probabilistic key distribution scheme for WSNs is the scheme called Random key pre-distribution (RKP) proposed by Eschenauer et al. [45]. In this scheme, each node i in the network is pre-charged randomly with a set of key ring of size k, let's R_i the subset of pre-loaded keys on the node i, selected from a large pool S. After the deployment of sensor nodes, each node i broadcasts its keys' identifiers to its neighbors. The node i establishes a key session between some neighbor j only if the intersection between R_i and R_j contains at least one key ($R_i \cap R_j \neq \emptyset$), and thereby they choose one key among $R_i \cap R_j$ as a session key. In the case of ($R_i \cap R_j = \emptyset$), nodes i and j determine a secure path composed of secure links. The main drawbacks of this approach are its memory consumption required for keys storage and importantly its non resiliency against key compromise attacks. Indeed, if some nodes are compromised by an attacker, all the session keys that these nodes have established with their neighbors will be disclosed which corrupt fundamentally the security of the network. Some enhancements [27, 42] of the basic RKP scheme have been proposed; namely: Q-Composite scheme [27] enhances the resiliency of RKP by introducing additional requirements in order to establish session keys between nodes, basically two nodes i and j can establish a session key only if they share at least Q keys used to compute a pairwise key obtained by computing the hash of all the concatenated shared keys. In [42], Du et al. proposed a solution to overcome key storage issue of RKP by establishing only the necessary session keys. On the other hands, Blom's scheme [18] is also a very efficient scheme that is very suitable for WSNs and IoT as claimed by some researchers [53]. In Blom's scheme, the secret keys are vectors obtained by simple matrix multiplications. The idea is that, each node i has an identifier I_i randomly generated and known by all nodes in the network. In the deployment phase, private key g_i for the node i is generated from its identifier as follows: $g_i = DI_i$, where D is a secret symmetric matrix generated over the finite field $GF(p)$ and p is a prime. For the node i, in order to share a secret key with node j, it computes $secret_{ij} = g_i^t I_j = g_j^t I_i$. Obviously the security of the scheme is strongly dependent of the secret matrix D which must be kept carefully by a central trust server and used also to add sensor nodes to the network.

Most of the key management solutions proposed in the literature have been designed for Wireless Sensor Networks but very few works were proposed initially to meet directly the security requirements in IoT. Recently, Sicari et al. investigated

[5] path composed from a set of successive secure links

a key management issue in distributed and dynamic Internet of Things environments [114]. They integrated two key management solutions (Dini et al. [40] and Di Pietro et al. [39] schemes) in their middleware based IoT architecture named NOS (NetwOrked Smart object) which has been designed initially as a distributed platform for data storage and processing between IoT devices that act as data sources and the users that act as services consumers [102, 112].

5.1.2. Traditional Public key solutions

Traditional Asymmetric approaches group all methods based on public keys and requires the authority to issue certificates to different users in the system. In this family, we find RSA, DSA, El Gammal, NTRU, ECC cryptosystems, etc. The advantages of these approaches are their flexibility, scalability and key management efficiency. However, these solutions are energy-consuming which are not suitable for constrained devices. NTRU consists of the less computational asymmetric approach based on the shortest vector problem in a lattice [94], however it requires more memory space to store keys. Elliptic curves are also in some cases very efficient and can ensure the same level of security as RSA and similar asymmetric cryptographic approaches with keys of small sizes [28]. Indeed, with 80-bit security level, we need only keys of 160 bit contrary to RSA where we need keys of 1024 bits.

The contribution in [81] is twofold. First a signcryption called DQAC scheme has been designed to sign and encrypt query messages which ensures authentication and confidentiality and it also preserves the privacy of users requesting WSNs' data. Second, a distributed access control based on the proposed signcryption scheme in addition to proxy based signature in order to anonymize users' identities. The proposed signcryption technique is based on Elliptic curve and is securely provable under the Computational Diffie-Hellman model.

The authors in [60] considered network users as a set of predefined groups, where each user is assigned to a single group. The groups are constructed in such a way users having the same access privileges belong to the same group. The main proposal consists on "privacy-preserving" ring signature scheme considering the members of each group as the nodes forming the ring. This technique allows IoT devices (signature verifiers) to grant access to legitimate users (signers) without disclosing the identity of each user neither from sensor data owner nor from other users. The only revealed information about queries is the group (gid) containing the signer's group ID from which the query is originated without knowing exactly which signer. The experiments were performed in real Imote2 platform running TinyOS [6] demonstrate the efficiency and feasibility of the scheme in real WSN and IoT applications.

In [56], authors claimed that, actually, existing access control mechanisms like RBAC (Role Based Access control), MAC (Mandatory Access control) are not anymore scalable, difficult to manage and don't fit well with distributed environments like Internet of Things, and hence the need for a new effective access control mechanism is unavoidable. The authors proposed a new access control mechanism called capability-based access control (CapBAC), which can overcome the actual issues in terms of scalability and manageability raised with the existing access mechanisms. The idea behind the concept is the usage of capability based authority tokens which are unfalsifiable and easy to communicate and grant seamlessly the access to IoT resources and process.

5.1.3. Identity Based Encryption (IBE)

The main issue of transitional public key cryptosystems is that they are not scalable enough. Indeed, they strongly depend on the authority that issues certificates for each user in the system which is required in order to deal with spoofing and identity usurpation. Therefore, certificates raise the complexity of the system. In order to overcome the scalability and the complexity issues, Identity Based Encryption tools have been proposed by introducing a new concept that consists to use unforgeable string related to the user identity (such as user's phone number, email address, etc.) as public key to encrypt data and thereby eliminate the need for certificates. Although their scalability and efficiency, IBE techniques are not very suitable for IoT because they are expensive and incur heavy resource consumption. In the literature, some research works have been investigated to design new, efficient, and lightweight IBE schemes that could support constrained devices.

Using Elliptic Curve Cryptosystems, bilinear maps and hash functions, Chen [29] proposed a new lightweight Identity Based Encryption scheme to secure communications between devices based RFID tags. The main advantage of the scheme is its simplicity and its ability to reduce substantially the computation overhead. However, the authors did not provide any discussion about the security of the scheme.

Fagen et al. [77] addressed the access control problem in WSN in the context of IoT where internet hosts query WSN to get sensor information. The main contribution consists of heterogeneous signcryption (HSC) technique based on two mechanisms: (1) certificateless cryptography (non usage of certificates) that belongs to internet hosts; and (2) IBC cryptographic technique that belongs to WSN environment. As singcryption technique, the proposed scheme ensures both authenticity and confidentiality with less computation. Moreover, it is useful to control the access between heterogeneous environments.

In [70], a signcryption scheme has specially designed for WSNs in the context of Internet of Things. The scheme is based on elliptic curves and is secure under the Diffie-Hellman computation hypothesis. Nevertheless, this scheme is applied only in contexts where the verifiers are always powerful nodes that have enough computational resources and it's consequently very heavy for IoT devices.

Fuzzy identity-based Encryption (FIBE) is considered as an enhancement of IBE with introducing error-tolerance property. The main idea behind FIBE is to give the users, having at least k among n attributes, the possibility to decrypt the ciphertext encrypted under the hole attributes (n) [106]. In [86], the authors designed FIBE scheme based on bilinear maps which

[6] embedded, component-based operating system: http://tinyos.stanford.edu/tinyos-wiki/index.php/TinyOS_Documentation_Wiki

is securely provable in the full model. Performance analysis demonstrated the applicability of this scheme in IoT.

5.1.4. Attribute Based Encryption (ABE)

The concept of Attribute Based Encryption has been introduced, first, by Sahai and Waters in Advances in Cryptology EUROCRYPT 2005 [106] as an enhancement of Fuzzy Based Identity Encryption [19, 32]. ABE introduces an expressive way to control the access to private data using policy access structure that defines relationships between a set of attributes [7] used to encrypt data. In ABE system, Key Generation Server (KGS) generates for each legitimate user a private key based on its attributes, and also a public key used to encrypt data based on predefined policy. A legitimate user is able to decrypt data only if it holds the sufficient attributes that satisfy the policy.

- **Key Policy ABE (KP-ABE)**: In this scheme, the data owner defines an access structure A and encrypts data based on a set of attributes I. A user which wants to decrypt the cipher-text must holds the attributes that satisfy the access structure A to be able to derive the private key that decrypts the cipher-text [52] (see figure 4).
- **Cipher-text Policy ABE (CP-ABE)**: In this scheme, the encryption is based on the access structure A. A legitimate user is a user who holds a set of sufficient attributes I that satisfies the access structure (policy A) attached to the ciphertext [16] (see figure 5).

Attribute-Based Encryption is considered as a promising scheme for many applications such Cloud computing, multicast communication, M2M, etc. Particularly, in Internet of Things' applications, we need often efficient mechanisms that ensure fine-grained access control to IoT data based on the roles of the users in the IoT systems. We can take as an example, the Healthcare applications where EHRs (Electronic Healthcare Records) related to patients are only accessed by physicians and nurses based on their roles in the hospital institution. This is achieved by ABE thanks to its scalability, efficiency and its fine-grained capability. However, the complexity and the high overhead induced by the cryptographic operations in ABE schemes make its application in resource-constrained devices very difficult. These drawbacks are serious problems to overcome in order to adapt ABE in IoT applications.

In [124], the authors proposed a distributed lightweight ABE solution based on CP-ABE scheme. The solution takes advantage of IoT heterogeneous nature which consists to delegate the most costly cryptographic operations (exponentiation) to more powerful nodes. However the solution consumes a lot of bandwidth, as objects exchange cryptographic information in order to accomplish the encryption process. The cost due to message exchanges is very considerable in the radio field and must not be neglected.

[7] properties related to the users in the system, for example: PhD student can be considered as an attribute

On the other hand, Nouha et al. [99] proposed ABE based solution that ensures a tradeoff between computation and storage capacity of constrained devices. They use a pre-computation technique in order to reduce computation cost. This technique consists to pre-compute and store in a lookup table a set of pairs obtained generally with expensive cryptographic operations done on elliptic curves and pairing group settings. This information is used later to carry out cryptographic operations with very low computations. The main drawback of this solution is that the look-up table must be as bigger as possible in order to overcome dictionary attacks.

Shucheng et al. [133] proposed a distributed fine-grained access control scheme based on KP-ABE for wireless sensor networks called FDAC. The authors consider sensor node properties such as its geographic location, the type of sensor's data, time, its owner, etc. as attributes to define access policies in order to control the access of users to sensor data encrypted under the defined attributes. The main properties of the scheme are that sensor nodes may change seamlessly their attributes as well as its capacity to support data aggregation. The feasibility of the solution is evaluated with real experiments under iMote2 platform.

In [54], the authors addressed the key storage in CP-ABE in IoT context. Mostly the encryption key is constant-size (does not depend on the number of attributes). The proposed solution is provably secure in the selective security model. However, this solution generates big ciphertexts which create a big problem for IoT devices that are highly constrained in terms of bandwidth and storage.

In contrast, Müller et al. in [92] proposed a multi-distributed-authorities based ABE solution for IoT environments. The solution is kind of an adaptation of ABE to support a distributed access policy among a set of authorities, where the generation of secret keys from the attributes is handled with the collaboration of several authorities. Each authority generates a sub-key taking in consideration its maintained access policy.

The most existing ABE schemes are based on expensive bilinear pairing operations, which are, in general, not suitable for constrained devices in IoT. For this reason, some researches have been conducted in order to propose a lightweight non-pairing ABE schemes. The contribution in [132] is new lightweight ECC-Based ABE scheme that consists on replacing pairing operations by point scalar multiplication on elliptic curves. Under the ECDDH assumption, the authors proposed a security proof of the scheme in the attribute based selective-set model.

In [118], the authors tackled the problem of integrity and authentication in IoT with an expressive attribute based signature (ABS) scheme. The scheme preserves the privacy of signers and don't leak any information about users. However the scheme is still heavy computational for both the signer and the signature's checker as it uses a lot of pairing operations and exponential computations. Thus the scheme is not quite suitable for IoT constrained devices.

In the context of communication based groups in IoT, the authors in [121] proposed to combine Attribute Based Encryption schemes and Publish Subcribe based MQTT messaging architecture in order to ensure data encryption as well as the se-

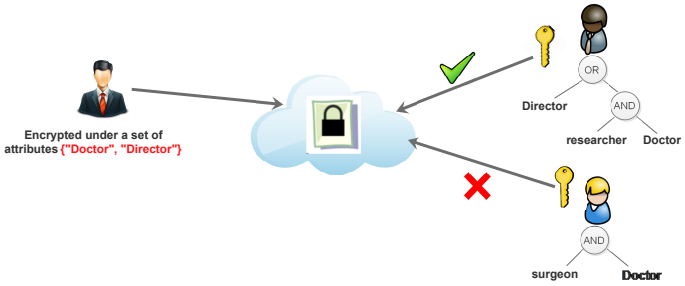

Fig. 4. Key Policy ABE (KP-ABE).

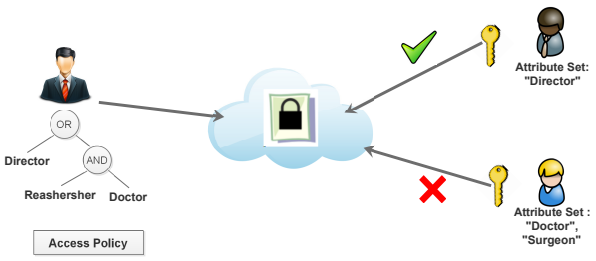

Fig. 5. Ciphertext Policy ABE (CP-ABE).

curity requirements in group communications, namely forward and backward secrecy. the proposed solution ensures a flexible keys updating in case of join/leave procedures in MQTT architecture.

In order to study the adaptability and feasibility of applying ABE schemes, namely CP-ABE and KP-ABE, on smartphone and IoT devices, Ambrosin et al. [9] have conducted intensive experiments in diverse mobile platforms (smart-phones, laptops, etc.) based on different OS (Android, Windows). The obtained results demonstrate the feasibility of ABE in smartphones and similarly for IoT devices. On the other hand, authors in [1] proposed a lightweight hardware implementation of CP-ABE scheme on Field Programmable Gate Array (FPGA). As a proof of concept, CP-ABE based 16 bits key size was tested with different setups. It's worth noting that with the conducted experiments, the scheme is quiet less power consuming.

5.2. Privacy solutions

Actually preserving privacy in IoT is mandatory as data issued by smart objects are very sensitives and inherently related to real life's individuals. The main goal of privacy techniques is to ensure the following requirements:

- **Anonymity**: Property ensuring that a third entity is unable to identify person's identity among other identities in the system.
- **Unlinkability**: Impossibility to cover the persons' identity from the information they produce.
- **Untraceability**: Difficulty to track actions and information issued from the behavior of an entity in the system.

The privacy solutions aim to protect sensitive data and also provide mechanisms that hide users' identities in such way the intruders cannot know about their behaviors. In the following, we discuss some solutions proposed in the literature that address the privacy of data and user's behaviors in Internet of Things.

5.2.1. Data privacy

Data tagging is one of the most known techniques, mainly used to ensure privacy of data flows. The idea behind this concept is to associate additional labels called tags, to data flows in order to allow trusted computing entities to reason about flows of private data and thus hide identities of individuals who hold or control data [21]. Nevertheless, tagging mechanisms might cause a challenge for constrained devices as tags' sizes raise according to the size of data and also generate additional expensive computations. In [47], authors demonstrated the applicability of tagging mechanism for constrained programmable micro-controller (PIC) by providing lightweight code templates dedicated to resource-constrained devices in order to add tags to data flows.

ZKP (Zero Knowledge Proof) is a powerful mechanism largely used to ensure the privacy of users' identities. The idea behind ZKP is to allow to one party (prover) to demonstrate to another party (verifier) some property by proving its possessing of some information without disclosing it [28]. This concept is very useful to develop security protocols while preserving the privacy of users' data and properties. In contrast, Ioannis et al. [28] proposed an evaluation of some ZKP protocols based on the Discrete Logarithm Problem on elliptic curves (ECC) for resource-constrained devices. The obtained results demonstrate that using ECC (with 1024 key's length) comparing to RSA provide less execution time and less memory with the same level of security. Importantly, with small message sizes, the energy related to the communication is minimized. However, beyond some threshold, the ZKP protocols became more overloaded which is due to the fragmentation of messages.

K-anonymity model is another potential approach to protect the privacy of data in Internet of Things' applications. Considering the context of a set of homogenous data stored in a table where each column represents a record of these data which is owned by some specific user. The K-anonymity models aim to protect each record in the table and make it indistinguishable from at least $k - 1$ records in the same table by hiding the sensitive information about its owner [119]. These sensitive information may be the ages, the phone numbers, the addresses, etc. This model is largely adopted in big data and cloud applications to protect the privacy of data streams issued by different users. Particularly, in IoT applications, there are also some attempts to adopt k-anonymity models [95, 63, 65]. In [63], authors proposed context aware k-anonymity model with conjunction to other privacy protection mechanisms to protect data issued from sensor nodes in WSN. Huo-wang et al. [65] investigated a clustering technique to propose a k-anonymity model to hide sensitive data about the locations of sensor nodes in IoT context. The idea behind the solution is to gather the data related to the sensor nodes located in different regions in different

classes to make them indistinguishable.

5.2.2. Privacy of users' behaviors

In Internet of Things, users and objects perform actions in the systems such as access to sensor data, control remote actuators, etc. Therefore, it's mandatory that their behaviors should be protected against malicious intruders. In what follows, we discuss some works that aim to protect the privacy of users' behaviors.

In [136], the main contribution is a privacy-aware access control protocol called DP^2AC in Wireless Sensor Networks based on RSA blind signature mechanism. In this solution, the owner of data signs the hash of an arbitrary integer m generated by some user x which forms an access token. So, the user x uses the token $< m, (\sigma(m) = (h(m))^d$, where $h(m)$ and $\sigma(m)$ are respectively the hash of the integer m and the signature of the message m using the owner's private key $d >$ to prove its capability to access data. The verifier which holds the data, checks if $h(m) = \sigma(m)^e = h(m)^{ed}$ to control the access of the user x without necessarily leaking any information about its identity. The protocol has the advantage to be simple and efficient. However, it does not ensure fine grained access as all users have the same privileges to access sensor data.

According to [34], decentralized approaches can enhance privacy more than centralized approaches as they do not rely to any central entity which might track data flows and thus can probably deduce sensitive information of individuals from the exchanged data. In contrast, Alcaide et al. [7] proposed a fully decentralized authentication protocol that preserves the privacy of users. Besides, users in the system are authenticated by data collectors in a flexible manner based on Anonymous Access Credentials which are unlinkable.

In [117], authors proposed a capability-based access control mechanism by introducing lightweight tokens to access CoAP [8] (Constrained Application Protocol) IoT resources while preserving the privacy of data over end-to-end communications. The token is exchanged in GET CoAP requests and contains the necessary information to control the access to device resources such as request Id, subject Id, Device Id, Issuer Id, Issued time, ESDSA signature, etc.

Recently, Samet et al. [123] investigated a new mechanism based on Data Obfuscation schemes in order to preserve the privacy of the exchanged metrics in smart grid AMI networks. The idea of data obfuscation is that each gateway creates and distributes obfuscated values to smart meters. Then, smart meters slightly disturb the sensed data based on obfuscated values and transmit them again to the utility control center, which can do estimation about the received data containing basically the electricity consumption of smart meters. This solution is less-computational which makes it applicable in resource-constrained devices. However, it generates a lot of overhead in the AMI network infrastructure.

[8] Considered as an alternative of HTTP in IoT environments

5.3. Availability solutions

In IoT, the availability of the system is one of the most important security services needs to be protected against malicious attacks (like DoS/DDoS) or unintentional failures. Very often, the damages caused by the violation of the availability are tremendous which can be economical losses (in manufacturing systems) or safety damages (in transportation systems). Furthermore, ensuring the availability is a very challenging task because attackers exploit all types of vulnerabilities in different levels (network, software design, cryptographic algorithms, etc.) to break the system. For example, in October 21, 2016, one of the largest American computer companies providing DNS service, DYN (Dyn Managed DNS) was attacked by hackers who used a type of DDos attack exploiting IoT devices. During this attack, many known sites were blocked for 10 hours, such as Amazon, BBC, PayPal, etc. The attackers take advantage of comprised IoT devices (such as surveillance cameras) infected with the malicious software named Mirai to relay massive packet streams.

5.3.1. IoT DoS/DDoS countermeasure approaches

IP Traceback methods are powerful mechanisms largely adopted in IP based networks such as Internet to detect DoS and IP flooding attacks in real-time. These methods focus mainly to enhance the security of IP based lightweight protocols basically designed as adaptations of the traditional TCP/IP protocols in the Internet of Things. DTLS [9] (Datagram Transport Layer Security), 6LoWPAN [10] (IPv6 Low power Wireless Personal Area Networks), RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks)) are just examples among other protocols widely adopted in the world of IoT which provide confidentiality and integrity of end-to-end exchanged information between IoT devices [107]. However, these protocols are not initially designed to deal with the most common IP based DoS/DDoS attacks. Many solutions have been investigated to enhance DTLS based transport layer and RPL based 6LoWPAN routing protocol in order to turn them more robust and secure against DoS attacks. In these solutions, IP routers and IoT gateways inspect and analyze packets in order to identify eventual malicious behaviors and take actions accordingly.

Regarding TCP/IP transport layer, the contribution in [84] consists on an enhancement of the DTLS protocol in order to mitigate DoS/DDoS against IoT devices and gateways. The enhancement is done by extending the process of the DTLS handshake with an additional cookie exchange technique where the server, before resource reservation, sends an authentication cookie's code to the client through *HelloVerifyRequest* message. This later, upon receiving the message, could authenticate the server and sends again to the server a new authentication cookie encapsulated in *Hello* message. To prevent IP spoofing attacks during the handshake phase, a mutual authentication step is done between the client and the server through a Gateway.

[9] An alternative standard of TLS, it is a UDP-based protocol which is less network overloaded

[10] Lightweight based IPv6 protocol to address IoT devices

On the other hand, in TCP/IP network layer and specifically in the routing level, many security enhancements of RPL and 6LoWPAN based IoT architectures are proposed. In contrast, Kasinathan et al. [67] proposed an architecture to protect IoT based 6LoWPAN devices against DoS attacks as well as jamming and tampering attacks in the context of the European project called *ebbits* [11]. The main contribution is twofold: first, the design of Intrusion detection manager that is charged to protect constrained devices against DoS attacks. Second, the design of the IDS (Intrusion Detection System), operating in promiscuous mode, that is responsible to monitor 6LoWPAN packets and raises alerts in case of any misbehavior. The solution is based on Suricata IDS [12] that uses the signature based detection technique. Likewise, Hummen et al. [64] investigated the attacks related to 6LoWPAN fragmentation mechanism, basically two attacks were studied: fragment duplication attacks and buffer reservation attacks which both of them aim to prevent the availability of the IoT devices. They proposed a mitigation approaches that counter to these attacks. In the routing level, Rghioui et al. [101] surveyed the potential DoS attacks that could disturb RPL and 6LoWPAN IoT protocols. They proposed also mitigation solutions of theses attacks based on IDS approach. Likewise, recently, [109] focused on intrusion detection in RPL based 6LoWPAN. They proposed some extensions of the protocol by exploiting the ETX (Expected Transmissions) metric as a mechanism to prevent malicious nodes.

Recently, Cusack et al. [35] discussed and compared many IP traceback approaches based on some metrics such as storage requirements, processing overhead, bandwidth overhead, scalability, etc.

Artificial intelligence techniques such as Artificial Neural Networks (ANN) are considered as one of the most powerful techniques used to design efficient IDS. For example, in [37], authors investigated the application of ANN to detect DoS attacks in IoT. Two kinds of ANNs were evaluated, namely : 1) Multilayer Perceptron with Limited Weights and 2) Multilayer Perceptron with normal weights in order to verify which one is more adequate as an IDS in IoT. It's worth noting that both of ANN techniques reduce false positive detection under training process, however they consume a lot of memory which makes them not quite suitable for constrained IoT devices.

Others researchers [82] investigated the possibility of applying Cumulative Sum (CUMSUM) algorithm in order to detect DDoS attacks in the context of IoT. The main aim of CUSUM algorithm is to detect real time changes in statistic process issued from data streams. The DDoS detection is done by analyzing the network traffic and computing statistics about it. The algorithm handles, continuously, these statistics to eventually detect changes which are related to any misbehavior in the network traffic. A trade-off between False Positive Rate and Detection Rate is also investigated by playing on CUMSUM algorithm parameters.

Other works have tackled with DoS attacks related to routing protocols in WSN and Internet of Things. Indeed, security of routing protocols is a fundamental field of research as many IoT applications use in general wireless mesh or ad-hoc network infrastructures to exchange data in real time. It is the case, for example, of AMI in smart grids and ad-hoc infrastructures in Vehicular Networks. In [6], authors interested in healthcare applications. They studied several mesh routing protocols in order to choose the most robust and secure protocol against DoS attacks. They focused on one type of DoS attacks that aims to divert the routing protocol behavior from its initial function. For example, routing attacks that force some network nodes to reroute data to inappropriate destination. Simulation results confirmed that PASER protocol is the most suitable for Healthcare applications and it is resilient against Hello Flooding attacks.

5.4. Discussion

In table 4, we present an application-centric classification of cryptographic based security solutions in IoT. Overall, we note that classical security solutions presented in this section are efficient in terms of optimization of resources such as computation, memory and bandwidth, however they don't meet scalability, heterogeneity and mobility challenges.

6. New emerging security solutions for Internet of Things

Internet of things promises to connect everything together anywhere and everywhere. All devices must interact efficiently with each other in a secure, scalable and reliable ways. Actually with the current centralized architecture, it could be difficult and challenging to deal with scalability in huge IoT networks. This issue may be solved by adopting a new approach of security emerged away from the current centralized model. New emerging approaches deal very efficiently with scalability, interoperability and compatibility issues. Hereafter, we discuss two emerging technologies which are being adopted as approaches to ensure security in IoT environments and deal very efficiently with scalability issues.

6.1. Software Defined Networking based solutions

The Software Defined Networking (SDN) is a new paradigm that has revolutionized the world of networks, thanks to the programmability and the intelligence it has introduced into the network. The main idea behind this concept, which began in 2011, is to separate the network control plan and the data plan. Using this paradigm, we can do centralized control and configuration of networks as well as dynamic management of network traffic. In SDN architectures, devices (routers, switches, gateways and IoT devices in general) do not make control decisions like forwarding tables and ACL rules [62]. Instead of that, they learn these rules from central component called SDN controller, which is managed to take all decisions in the network using protocols like Openflow. Devices in SDN architecture handle packets based on flow tables dictated by SDN controller. A typical SDN architecture is depicted in the figure 6.

SDN is an efficient solution to meet some challenges in IoT environments where most of devices have limited network

[11] https://www.fit.fraunhofer.de/en/fb/ucc/projects/ebbits.html
[12] https://suricata-ids.org/

Table 4
Classification of Classical based security solutions in IoT applications.

Applications \ Challenges		Computation complexity	Communication complexity	Memory	Mobility	Heterogeneity	Scalability	Quality of Service
Smart Grids	**Confidentiality**	[99], [54]	[54]	[99], [124]	-	[99], [124]	[99]	[99]
	Privacy	[47], [7], [63]	[7], [63]	[47], [7]	-	[123]	-	-
	Availability	[35], [84]	-	[84], [35]	-	-	-	-
Smart cities	**Confidentiality**	[99], [124]	[99], [118]	[99], [118], [124]	-	[124]	-	-
	Privacy	[7], [63]	[7]	[63]	-	[63]	-	-
	Availability	[67]	[67]	[67]	[67]	[67]	-	-
Transport	**Confidentiality**	[99], [54], [121]	[99], [118]	[124], [54], [121]	-	-	[54]	-
	Privacy	[47], [7], [63]	[7], [63]	[47], [7]	-	-	-	-
	Availability	[6]	[6]	[6]	-	-	[6]	-
Manufacturing	**Confidentiality**	[124], [99], [132], [118]	[99], [132], [118]	[124], [132], [118]	-	-	[99], [118]	-
	Privacy	[7], [63]	[7], [63]	[47], [7]	-	-	-	-
	Availability	[6], [67]	-	[6], [67]	-	-	[6]	-
Healthcare	**Confidentiality**	[124], [54], [99]	[54]	[124], [54]	-	-	[54]	-
	Privacy	[47], [136], [7]	[47], [136], [7]	[47], [136], [7]	-	-	-	-
	Availability	[67], [82], [6]	[82], [6]	[67], [6]	-	-	[6]	-

In this table, we provide an application-centric classification where we consider each IoT application separately and enumerate the sub-set of the solutions that should be applied and more suitable for this application. We investigate also how much each solution is efficient to deal with the different challenges.

resources. As a result, SDN deployment in conjunction with NFV (Network function Visualization) can optimize efficiently the resource allocation in IoT devices. Therefore, it introduces some many opportunities in order to overcome some challenges of reliability, security, scalability and QoS in IoT applications in more efficient and flexible way [62]. Hereafter, we discuss some SDN based solutions that address the security issues in IoT.

The main contributions in [48] are twofold. First, the authors proposed a new multi-domains SDN based IoT architecture that supports both networks with or without infrastructure. Second, they designed a distributed security model to manage security policies between multiple SDN domains. In order to address the conflict issues that appear from the enforcement of the security policies on the several domains, the solution takes advantage of the grid of security paradigm that aims to solve security heterogeneity issues. So, each SDN controller is charged to push security policies inside its domain and coordinates with other SDN controllers outside the domain.

In [24], authors presented an openflow [13] based SDN architecture for IoT devices. The proposed architecture includes IoT gateways that are managed to identify attacks and anomalies in order to determine which devices are acting maliciously and which are the compromised nodes in the network. To do that, each gateway analyzes the network traffic dynamically. So, upon the detection of an anomaly or an abnormal behavior such as generated periodic flows (DoS attacks), the gateway applies an appropriate mitigation action (block, forward, apply QoS) depending on the anomaly.

The work in [126] considers the heterogeneous IoT infrastructure as a couple of connected clusters or segments, where in each segment, there are IoT nodes that support Openflow protocol and have sufficient resources in terms of computation and energy. These IoT nodes act as SDN gateways, and are charged to: 1) authenticate nodes in the same segment, and 2) enforce adequate security rules using Openflow protocol. The SDN gateways exchange between them the security rules in order to establish secure, end-to-end connections between IoT nodes in

[13] The most known SDN protocols, proposed by ONF

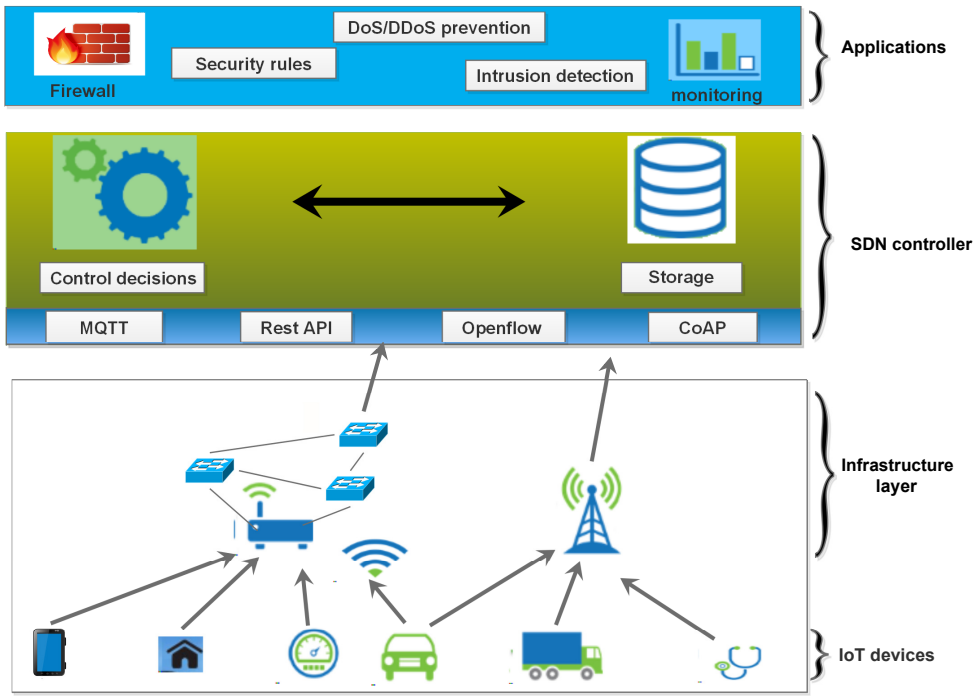

Fig. 6. Software Defined Networking architecture for Internet of Things.

different segments.

Gonzalez et al. [51] present a new SDN framework to overcome the different kind of attacks in IoT environments. The proposed framework is based on the architecture called SDCSN (Software Defined Cluster Sensor Networks) proposed in [97] that consists of multi-domain SDN architecture. Each SDN domain (cluster) has a SDNCH (SDN Cluster Head) that is charged to monitor and secure SDN domain and prevent outside and inside attacks. The mechanisms employed in order to implement an SDN firewall are based on analysis of flow entries on the application level.

Other works investigated SDN approaches as solutions to prevent against malicious attacks such as DoS and also implement efficient IDS. In this contrast, Lee et al. [75] tackled the problem of availability in IoT based gateway environments for which they proposed an SDN based solution to prevent IoT gateways from DoS attacks and evaluate the main impacts. In order to evaluate the impact of different kinds of Dos attacks on IoT gateways, the software solution was implemented using Raspeberry Pi2 platform, OpenWRT operating system as a wireless Router and Opendaylight as an SDN controller.

Aydeger et al. [12] proposed a SDN-based MTD (moving target defense) mechanism to defend against specific types of DDoS attacks called Crossfire. The SDN-based mitigation approach consists to enhance the packet forwarding process in such away routes containing congested links are avoided.

6.1.1. Main challenges of SDN in terms of security in IoT

During these last years, there are a lot of discussions about SDN and its benefits in the industry of networking. However as new emerging technology, SDN is not enough mature to address the security issues in Internet of Things. Hereafter, we discuss some potential challenges that are still difficult to overcome with SDN based approaches:

- In general SDN based security solutions are designed to operate in centralized architectures. Therefore, the centralized SDN controllers emerge as a potential single points of attacks that should be protected against attacks such as DDoS for example.
- Southbound interface between SDN controller and data plan is vulnerable to threats that could degrade the performance of the network. As example, Openflow protocol suffers from integrity as mentioned in [20].
- SDN approaches suffer from scalability issues. Indeed, SDN controllers can not deal efficiently with the large number of IoT devices in the underlying data plan network.
- In highly dynamic environments like vehicular networks, where network topology changes frequently and a lot of messages are exchanged between vehicles, centralized SDN approaches is still limited. Indeed, gathering all these changes from the underlying network to enforce security policies and configurations using SDN approaches takes a lot of time.

6.1.2. Discussion

In the light of the analysis of the different SDN based security solutions, we provide in table 5 a comparison between these solutions with respect to the parameters : resources consumptions (computation, memory and communication) as well as mobility, heterogeneity, quality of service and scalability. It's

worth mentioning that SDN solutions are more convenient in some applications and deal efficiently with quality of service and heterogeneity issues. However, in most situations, they suffer from scalability issues regarding their centralized architecture.

6.2. Blockchain based solutions

Blockchain is a new effective technology that has revolutionized the world of cryptocurrency. It consists mainly of a secure distributed database (a.k.a public ledger) containing all transactions have been made by all the participating entities. In cryptocurrency blockchain based solutions such as bitcoin and ethereum, transactions are done and validated in a distributed peer to peer infrastructure. Basically, when an entity A wants to carry out a transaction with another entity B, it sends a transaction request to all the peers in the blockchain netwok. Then, each node collects, periodically (10 minutes in the case of bitcoin), a set of transactions and groups them in a single block. Finally, the process of validation of each block is done in a distributed way using a consensus algorithm that is executed by some nodes in the network, called miners. In figure 7, we illustrate the different steps evolved in the blockchain transaction treatment process.

New emerging IoT based applications will be taking advantage of secure and private transaction messaging, decentralization of communications, privacy by design which are all very important features for industrial internet and Internet of Things in general [13]. As IoT continues to grow, sensors and devices are becoming more common places to communicate information like location, temperature and other properties. Often, this information needs to be shared between different entities and exploited for big data analysis and also for monitoring purposes in some critical applications. Blockchain can help to create tamper-resistant record which allows all participating smart objects to access the same data in more consistent and safer way. In addition to data flow management, blockchain consists of an efficient way for automating business and creating smart contacts among smart devices without referring to central entities. We mean by smart contracts, all kinds of digital rules forming the terms of contact [31]. Concretely, a smart contract consists of a computer program that is automatically executed by smart objects, and defines a set of rules and conditions based on the terms of the contract. Blockchain could help to ensure the smooth running of the contracts in a distributed way.

Blockchain technology has received a great attention by researchers in various fields. Until now, its application has recognized a great success in financial applications and smart contracts, but some researchers claim that it's worth investigating to think out of the box and try to figure out other application domains than cryptocurrency that this effective technology can improve considerably as Internet of things and security domains. Indeed, we already have some examples of applications that are non financial such as global identity registry systems (namecoin [79], Blockstack [8] among others), insurance applications [83], online voting [103], supply chain provenance [69], decentralized peer to peer storage platform (storj [130]) etc. Moreover, recently, in the literature, some blockchain based solutions have been proposed to solve some security and privacy issues in IoT. We discuss some of these solution in the following sections.

6.2.1. Benefits of blockchain in IoT

Hereafter, some added values that blockchain technology can bring to IoT and security domains [34]:

- **Decentralization**: Because of the decentralized architecture of IoT, blockchain is most suitable as a security solution in IoT. The decentralized architecture of blockchain makes security solutions most scalable and can solve the problem of single point of failure and becomes more robust to DoS attacks.
- **Pseudononymity**: The nodes in blockchain are identified by their public keys (or the hash of public keys). These pseudonyms don't link any information about the identity of the participating nodes.
- **Security of transactions**: Each transaction, before being sent to blockchain network, is signed by the node and must be verified and validated by miners. After the validation, it's practically impossible to forge or modify transactions already saved in the blockchain. This provides a proof of traceable events in the system.

6.2.2. Secure IoT transactions

Using blockchains, some works were focused on secure IoT transactions in decentralized architectures. We discuss hereafter some of those proposals.

The first IoT platform based blockchain solution was developed by IBM in 2013. This platform is called ADEPT (Autonomous Decentralized Peer-To-Peer Telemetry) [10] which consists of proof of concept of a decentralized and secure IoT platform based on Ethereum protocol which is a seamless solution to deal with devices contracting and transactions in a most scalable way. So IoT devices can define and set autonomously their own roles, responsibilities and permissions in the whole IoT ecosystem and also can do transactions and complex negotiations between themselves.

In [49], authors proposed an HTTPS protocol for IoT devices by eliminating the intermediary devices (like mobiles) to create secure HTTPS channel (classical solution). The session key is generated by PBKDF2 (Password-Based Key Derivation Function 2) algorithm and the IoT transactions are stored in a blockchain maintained between several devices. This solution could be enhanced by introducing a priority among transactions.

Recently, Kamanashis et al. [17] proposed a multi-layer security architecture for smart cities that integrates the blockchain as a distributed database layer to share and store heterogeneous IoT data related to the smart city environment such as traffic, temperature, location, humidity, etc. The data storage aims to share these data in a secure way among different smart cities'

Table 5
Classification of SDN based security solutions in IoT applications.

Applications \ Challenges	Computation complexity	Communication complexity	Memory	Mobility	Heterogeneity	Scalability	Quality of Service
Smart Grids	[48], [126], [51]	-	[48], [126]	-	[126]	[48]	[126], [51]
Smart cities	-	-	-	-	-	-	-
Transport	-	-	-	-	-	-	-
Manufacturing	[48], [126], [51]	[126]	[126], [51]	-	[126], [51]	-	[126], [51]
Healthcare	[48], [24], [126]	-	[48], [24], [126]	-	[126], [51]	[48]	[48], [24], [126]

The table provides a classification of SDN approaches with respect to the different challenges. Overall, the solutions are very efficient in terms of optimization of resources and ensure a high level of quality of service but they suffer from scalability and mobility issues.

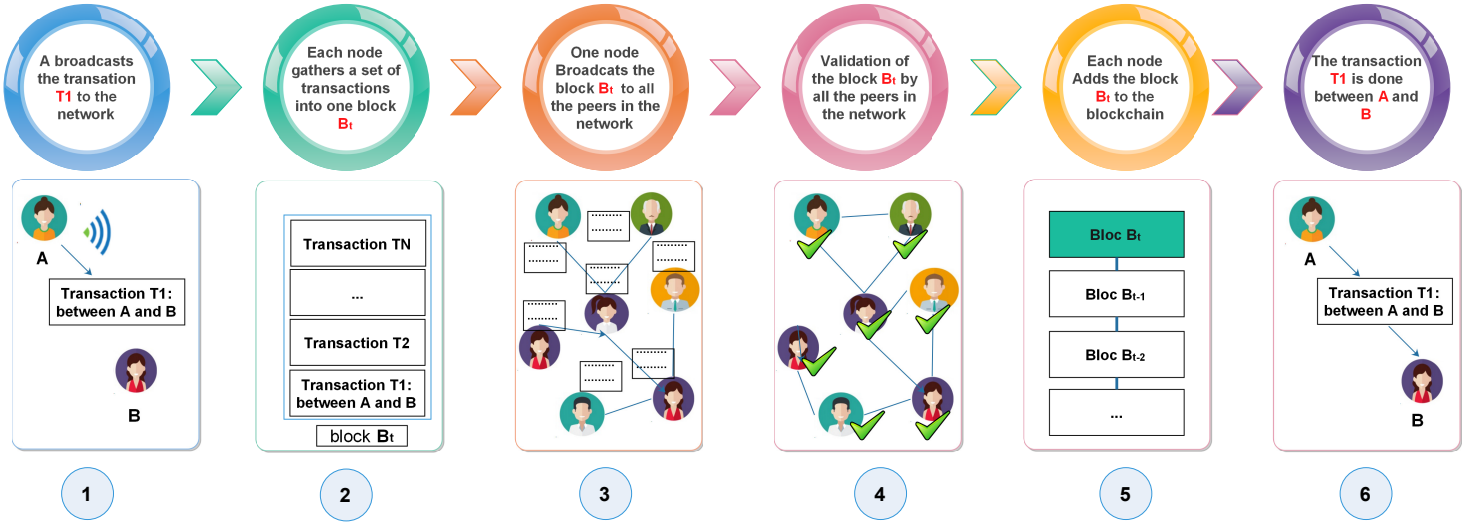

Fig. 7. Blockchain: steps of transactions' validation process.

components. The architecture is designed to deal with scalability and reliability issues that are very challenging in smart cities environments.

In [71], the authors proposed a solution to manage SSH public keys based on blockchain and collective signing authorities. They mainly addressed the key management problem presented between IoT devices to access to distant services. The main idea of the solution consists on adding a new block in the blockchain containing the SSH public keys whenever a key is added, rotated or updated.

Recently, Hardjono et al. [58] proposed a solution for identifying the manufacturing provenance of IoT devices while preserving the identities of the users using blockchain and cloud computing. The authors proposed a platform solution based on EPID (Enhanced Privacy Identity protocol) of Intel, a standard used for identification of IoT devices. The platform supports also device owners data selling in order to incentive IoT devices' owners to share their IoT data.

6.2.3. *Data Sharing*

In several IoT applications, a lot of data is exchanged between objects and with other entities. For that, it's very important to deal with these data and propose security solutions to share it with others. Moreover, privacy is a great issue that should be considered while addressing sharing data problem in IoT. According to [34], to ensure privacy in IoT systems, it is recommended to use peer-to-peer architecture, and specifically the blockchain technology. In addition, as all the operations handled on IoT data are controlled by the blockchain, it is easy to detect any abuse in data [34]. Blockchain might serve as a tool to deal with all these aspects. In this trend, several works have been proposed.

In [59], authors proposed a decentralized solution for sharing data in IoT environment which consists of a distributed data storage system. The proposed system uses blockchain to maintain data access control and data storage model. The main features of this system are: 1) separation of data store and data management. This later is ensured using blockchains, 2) a de-

centralized access control and 3) a scalable messaging based on Publish-subscribe model to query data.

In [134], authors proposed a healthcare data sharing based blockchain architecture. The proposed architecture includes three layers to manage the access to private ERH (Electronic Medical Record) related to patients. The first layer consists of the different users that are potentially interested to access the patient's data. To do that, a user sends different requests to the Healthcare Data Gateways (second layer) in charge of the management of the access control to the data stored in the blockchain, used as a storage data layer which is based on cloud storage. Besides the immutability property of blockchain, the ERH are encrypted and signed to ensure the confidentiality, the authenticity and the integrity of data.

6.2.4. Some interesting concrete applications of blockchain in IoT

In the following, we discuss some interesting blockchain based applications:

a) Alliance on IoT Blockchain (Guardtime and Intrinsic-ID) [14]: Intrinsic-ID is a company that proposes cryptographic solutions to authenticate embedded devices using technology called Physical Unclonable Function (PUF) which is largely used to protect sensitive operations like payments and data related to governments. The goal of Guardtime is to provide a security solution using essentially KSI (Keyless Signature Infrastructure) platform which consists basically of a scalable blockchain solution.

b) Chronicled.com [15]: It is a new startup whose main activity consists in developing blockchain based solutions for security problems, namely the identification and the authenticity of IoT devices. They claimed that current protection mechanisms such as QR codes, barcodes are easily forged and thus blockchain might solve those issues thanks to its tamper-resistant feature.

6.2.5. Main challenges of blockchain in IoT

Despite the blockchain's benefits mentioned above, it is still some challenges to be solved in order to adapt the blockchain technology in IoT. We enumerate the following challenges:

- **Computation and storage issues**: As most of IoT devices have limited capabilities in terms of computation and storage resources, the blockchain needs to be customized before its application as security solution in IoT. To address the problem of adaptability, one solution may consist to add a new application level that hides the details of blockchain implementation, namely the PoW (Proof of Work) [34]. This solution allows the resource-constrained IoT devices to involve in the system without computing the PoW.
- **Time latency**: In bitcoin blockchain, the validation of transactions takes about 10 minutes, which creates a problem for real time applications.
- **Scalability issues**: Although the remarkable success of bitcoin blockchain and the number of users that rises year after year, blockchain technology is still non scalable solution in IoT environments. Indeed, according to cisco, by 2020, more than 20 billion of IoT objects will be connected to Internet [46].
- **Bandwidth consumption**: As IoT devices generate a lot of transactions, this includes an important problem if it is necessary to validate each of those transactions that consume a lot of bandwidth.
- **The anonymity**: Actually, blockchain does't ensure a fully anonymous transactions. Indeed, the peers are identified by pseudonyms that can be tracked but they are still unlikable (impossibility of extracting identity of the person from its pseudonym) [34].

6.2.6. Discussion

To summarize, currently, the works addressing the application of blockchain technology in IoT have covered only partial aspects of security. The research is still in its beginning. In table 6, we provide a comparison of the solutions based on blockchain technology. We note that the solutions deal efficiently with scalability and heterogeneity issues compared to previous approaches such as SDN and cryptographic tools. We believe that this technology will bring a lot of benefits to IoT security.

7. Context-awareness and security in IoT

Internet of things is a complex system that operates in dynamic environments that might be subject to real time variations. The heterogeneous nature of smart objects and the dynamic environment of Internet of things introduce new security requirements and challenges that should be considered. Therefore, the security solutions implemented in IoT should adapt to its dynamic environment and should be aware to the context in which smart objects evolve.

The context awareness plays a very important role to mitigate the different applications of IoT. The context can include any information about the environment such as objects' locations, temperature, the level of battery of each smart device, the level of sensitivity against attacks, and also the trustworthy of the IoT components. All these pieces of information are very useful, bring more values and enhance the decision process in the IoT applications and services. Besides the decision making process, context-awareness approaches participate also to enhance the security enforcement decisions based on the analysis conducted on the context. We can take as an example, wireless sensor energy constrained nodes that are equipped by sensor capabilities that allow them to measure information about the trustworthy level of neighbor nodes, on the fly, to forward sensitive data only to trusted neighbors. Furthermore, battery level of

[14] https://www.intrinsic-id.com/intrinsic-id-guardtime-announce-alliance-iotblockchain/

[15] http://chronicled.com/case-studies.html

Table 6
Classification of Blockchain based security solutions in IoT applications.

Applications \ Challenges	Computation complexity	Communication complexity	Memory	Mobility	Heterogeneity	Scalability	Quality of Service
Smart Grids	[17]	-	-	[17]	-	[17], [71]	-
Smart cities	[58], [49], [17]	[58], [49], [17]	[58], [49], [17]	[17]	[58], [17]	[58], [17]	-
Transport	[49], [17]	[49]	[49], [17]	-	-	[49], [17]	-
Manufacturing	[58], [59], [17]	[58], [49], [59]	[58], [49], [59]	-	[58]	[58], [49], [59]	-
Healthcare	[58], [17]	[58], [17]	[58], [17]	[58], [17]	[58]	-	-

The table provides a classification of Blockchain approaches with respect to the different challenges. Overall, Blockchain solutions address very efficiently scalability and heterogeneity issues thanks to their decentralized architecture.

sensor nodes could be an important factor to cope with the enforcement of security mechanisms such as encryption of sensor data. Consequently, the context measurement might be used as a mean to establish a trade-off between the energy-consumption and security level in IoT applications.

In the literature, there have been many works that have taken into account the context to develop security context adaptive solutions. Hereafter, we discuss some context-aware security works.

The contribution proposed in [57] is an adaptive security solution for IoT systems based on Markov game theory. First, they proposed a mathematical model representing the context of IoT environment based on three fundamental elements: energy consumption, communication and intruder models. Moreover, a game-theoretic model is proposed in order to ensure a trade-off between security and energy consumption that is a crucial challenge in IoT systems. Several adaptive security policies are tested. Their main goal is to determine the action each smart object have to perform according to its context (either it enables security services or disable it).

In [93], the authors proposed a framework that integrates some adaptive security solutions. The framework is based on the toolkit SetKit in order to enforce policies aiming to control the access to IoT data based on the the user's locations and context information. The main limitation of this approach is that the detection of the context does not consider the quality and the ambiguity of the collected data.

In other work, Di et al. [38] proposed an adaptive energy-aware security approach for Energy Harvesting Wireless Sensor Networks (EH-WSN). The main idea consists to adapt dynamically and autonomously, at each sensor node, the security parameters such as the cryptographic primitives, the size of the encryption key as a function of the level of the collected energy. The solution was implemented as an extension of ODMAC (On Demand Medium Access control) protocol.

The contribution in [128] consists of a framework called MDPAS based on Markovien Decision Process and aspect-oriented programming paradigm. The goal of this solution is to enable adaptive security solution that groups integrity, confidentiality and authenticity while making adequate decisions dynamically about the enforcement of security policies based on computing and energy contexts.

Hellaoui et al. [61] developed an adaptive security solution which considers the trustworthy of sensor devices in the Internet of Things. Each sensor node computes periodically the level of confidence of its neighbors based on its experiences with them and its own observations as well as recommendations obtained from other neighbors. The measured trust levels allow each node to decide dynamically whether it authenticates each of its neighbors or not.

In [120], Taddeo et al. proposed a solution that optimizes the energy consumption by establishing a trade-off between the security and the energy consumption while maintaining a certain level of Quality of Service (QoS) in the network. The solution consists to reduce the number of transmitted packets whenever the battery level of nodes is low by sending only the essential packets.

The authors in [112] proposed a distributed middle-ware based solution named NOS (NetwOrked Smart objects) which consists on a lightweight architecture to assess the level of security, integrity, sensitivity and also the quality of generated data in IoT environment. Different score levels are attached to each data source as meta-data by considering some requirements such as: accuracy, precision, integrity, confidentiality, authentication, etc. The advantage of this solution is its ability to deal with heterogeneous data sources in a distributed environment while addressing both of security and quality of data. As a demonstration, the authors developed a prototype based on Node.JS [16] and MongoDB [17] platforms, using Raspberry Pi

[16] nodejs.org/
[17] www.mongodb.org/

(executing the middle-ware), laptop (emulator of IoT devices) and a set of terminal devices as experimental setup.

7.1. Discussion

The context plays an important role to better address security challenges in dynamic IoT environments. In table 7, we provide a comparison of context-awareness solutions that we presented in this section. Overall, the solutions in this category meet efficiently performance requirements such as power consumption, computation, memory occupation and quality of service. However, compared to other techniques, these solutions remain less developed in the literature, especially in the context of IoT. Therefore, more research efforts should be devoted to fill the gap and enhance the existing solutions by taking advantage of the environment in which IoT devices evolve.

8. Safety and security in Industrial Internet of Things

As presented previously in section 3.5.2, safety is a common issue for many IoT applications like manufacturing systems, transport and also Healthcare based IoT applications among others. Safety issues could be produced in some cases from security attacks. In this section, we highlight the main relationships between safety the security and develop the main solutions to overcome both of the challenges jointly in Industrial based IoT systems.

8.1. Safety and security: definitions and relationships

Before discussing the main existing design approaches combining the safety and security in industrial infrastructures, we first define the two concepts and show the main differences and relationships between them.

We must point out that both safety and security deal with the risk concept which could be intentional or accidental and has a real impact at different levels: human, financial, environmental, etc. Often, safety is related to accidental risks originating from the system for examples: natural disasters or damages, material losses or damages, human errors, etc. However, security is related to malicious risks, performed by humans via malicious and intentional attacks which could be performed locally or remotely. In more clear and concise way, the safety of the system could be defined as an agreement that the system does not harm its environment, while the security of the system consists in protecting it from the intentional attacks that come from its environment [23]. From this definition, it is clear that the two concepts are deeply linked and one can impact the other. As an example, if the integrity of exchanged data between medical devices embedded in the body of a patient and his remote physician is compromised by security attacks, the physician could take decision to inject a wrong dosage in medical devices which could harm the patient and cause serious safety damages for his health.

In the figure 8, we demonstrate the main relations between safety and security in IoT systems which are in general context-aware in which Cyber-Physical systems evolve [72].

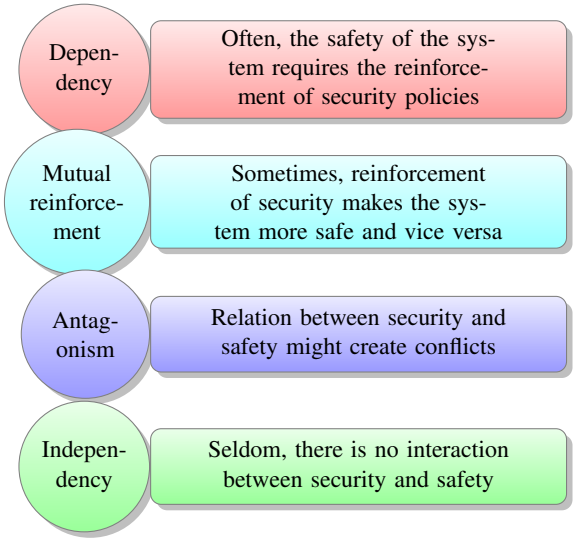

Fig. 8. Relationships between safety and security in Cyber-Physical Systems.

Basically, complexity is induced from the relationships between security and safety and also from the sensitivity of this later to accidental failures related to the safety and malicious attacks related to the security. This complexity created a real need to consider a single design approach which takes into consideration jointly security and safety.

8.2. Security and safety design approaches

In critical Cyber-Physical Systems, the safety and security were studied separately for a long time [72]. However, recently there were some investigations to integrate both of security and safety and study them jointly using a global design approach.

According to Eames et al. [44], there are basically two families of generic design approaches, namely:

- **a) Unification approaches**: They consist to model the requirements of both safety and security jointly without considering the different conflicts between them.
- **a) Integration approaches**: First, these approaches model the requirements of safety and security separately. Second, they investigate the different interactions between them in order to identity conflictual situations.

Formal and semi-formal approaches which are based on mathematical models and graphical tools are used in order to provide efficient tools to model interaction between security and safety. Stochastic tools such as Petri networks and Bayesian Belief Network (BBN) have been investigated in several works [90, 43]. They have been used to model the Cyber-Physical behaviors and assess risks on safety and vulnerabilities in terms of security. They have been also used to model the conditional dependencies between security and safety [43]. In addition, software modeling approaches such as UML [100, 116] and Model-based system engineering [22] approaches consist of graphical and semi-formal tools used to identify the requirements of the system in an architectural point of view by taking into account undesirable behaviors. Other formal approaches could be also

Table 7
Classification of Context-awareness based security solutions in IoT applications.

Challenges / Applications	Computation complexity	Communication complexity	Memory	Mobility	Heterogeneity	Scalability	Quality of Service
Smart Grids	[120]	[38]	[38]	-	[112]	-	[120], [112]
Smart cities	[57]	[57]	[57]	[57]	[112]	-	[120], [112]
Transport	[61]	[61]	[61]	[61]	[112]	-	[120], [112]
Manufacturing	[128],[128]	[38]	[38]	-	[112]	-	[120], [112]
Healthcare	[57],[128]	[57], [38]	[57], [38]	[57]	[112]	-	[57],[120], [112]

The table provides a classification of Context-awareness approaches with respect to the different challenges.

employed such as fault tree approach. In contrast, Silva et al. [115] proposed a tool based on fault tree formalism to evaluate the dependability (the reliability and availability) of Internet of Things' applications. The goal of such tool is to prevent system designers in their design stages to take early decisions in order to minimize faults in IoT systems before the deployment phase.

8.3. Secure Control mechanisms

Secure control problem in Cyber-Physical Systems deals with operational goals which basically consist on the set of features and goals that the system provides under the natural and normal conjectures [26]. As an example, one of the operational goals of smart grid system is the optimization of the production of electricity with respect the real consumption of each customer in real time. This goal is achieved based on remote commands exchanged between smart meters and control units. So, from security point of view, we should protect the execution of these commands from attacks aiming to tamper or alter them and thus prevent the achievement of the main goal which is the optimization of electricity production. The main aim of secure control mechanisms is to protect these operational goals from malicious party attacking Cyber-Physical infrastructure.

From Information security's point of view, there are three types of approaches to secure the control in Cyber-Physical systems [26]:

- **Proactive mechanisms**: It consists on preventive techniques that anticipate in order to mitigate data protection from malicious attacks. As examples of these mechanisms, we can cite the following mechanisms: authentication, access control, accountability, software security, redundancy, diversity, separation of privileges.

- **Reactive mechanisms**: It's also important to detect in real-time malicious attacks and react accordingly: detection and response. Intrusion detection systems, key revocation are some examples for reactive mechanisms.

- **Design and analysis principles**: They include the several preliminary theoretical analysis which allows to: decide if such security scheme is enough secure, define the adversary model to proof the security of different schemes, decide if an entity is trusted, etc.

8.3.1. Review of secure control approaches

In what follows, we discuss some proposed mechanisms to secure control in Cyber-Physical based IoT systems.

In [129], authors proposed a lightweight protocol to secure remote control of IoT devices by portal controllers like smart phones or tablets. The protocol is resistant to classical attacks such relay, DoS, desynchronization and man in the middle attacks and preserves the privacy of communications like non traceability of control messages between the smart devices and controllers. However, the protocol has some scalability issues, since each IoT device needs to share symmetric keys with trust center and all legitimate portal controllers controlling such device. In addition the protocol generates an overhead regarding the number of exchanged messages.

In [91], the authors propose a solution to detect replay attacks in Cyber-Physical systems and propose countermeasures guaranteeing the detection of these attacks under some predefined probability. They considered Linear Invariant control systems with Linear Quadratic Gaussian (LQG) controller. Basically LQG controller and Kalman filter used generally in those systems behave statically and thus are not quite adequate with dynamic systems. The idea behind the proposed solution is to redesign LQG controller to take in consideration the dynamic of the system to be able to detect dynamic attacks like relay and hijack attacks. The simulation results demonstrate that the rate detection converge asymptotically to 1 with respect to the filter window's length.

8.4. Discussion

Safety and security are real challenges in critical systems as the case of some IoT applications such as transport, industrial

systems, healthcare, etc. Both concepts are usually studied separately in these complex systems. However, with the rise of the interactions between safety and security in these systems, other emerging research trends have stimulated several researchers in both security and safety communities. Although, many efforts have been devoted to address the dependencies between safety and security using formal and modeling tools, this challenge is still significant which is due to the lack of standardization and the diversity of the scientific tools used in these two fields [72].

9. Summary and discussion

In Table 8, we present a comparison of security solutions implemented in IoT based on criteria that we described previously in section 3.6

At first glance, we notice that security solutions implemented in IoT and proposed in the literature are not all efficient in all the aspects and don't fulfill all the security requirements. Indeed, traditional solutions based on cryptographic techniques which are adapted for IoT applications are, generally, efficient in terms of storage and computation. However, they are limited in terms of scalability and heterogeneity. In the other hand, blockchain based solutions deal very well with scalability and heterogeneity issues thanks to the distributed architecture offered by blockchain technology. Nevertheless, the most drawbacks of blockchain technology are the energy consumption and latency caused by the proof of work mechanism to validate transactions which is serious problem in the case of real-time and energy constrained IoT applications. In the other side, SDN approaches optimize very efficiently computation costs, energy consumption and network resources since all control tasks are dedicated to high-performance servers (called SDN controllers) which discharge constrained IoT devices from greedy operations (including the execution of cryptographic tasks). Obviously, as a centralized approach, SDN doesn't deal efficiently with scalability issues in IoT.

9.1. Recent Trends and open security issues in IoT

In a high level synthetic picture, IoT still faces open issues that must be overcome. In the following, we provide some research trends.

Asymmetric cryptographic solutions proposed in IoT are very flexible and can deal with complexity and scalability issues. However, they are generally energy-consuming. So, several research works are investigating in order to optimize classical asymmetric approaches (ECC, RSA, NTRU, ABE, etc.). The main challenges is to establish a trade-off between security level and energy-consumption of the asymmetric cryptographic solutions. Indeed, solutions should ensure an acceptable level of security while reducing the energy consumption in IoT constrained devices.

Blockchain technology is considered as a promising technology that could offer a high level of security of IoT transactions. A lot of researchers believe that this technology could change the world of IoT in terms of security and services. Currently, this technology is still just in its early stage, and therefore a lot of research must be conducted in order to optimize some of its important features such as proof of work used to validate transactions and make it less consuming and more faster. In addition, Blockchain suffers also from some privacy issues and is still vulnerable to anonymity attacks [34]. In the Blockchain, pseudonyms are used as users' identifiers to send and receive transactions. In fact, the pseudonym does not ensure the privacy of transactions, it's still possible to de-anonymize a user and disclose its identity by analyzing transactions' inputs and outputs. Recently, several attempts have been investigated to address this issue. Mixing protocols [11, 15, 125] are considered as efficient techniques to fix this problem. The main idea behind these approaches is to provide mechanisms that allow users to send and receive transactions in such a way it's difficult for an attacker to find out the correspondence between input and output addresses of the same user. One such solution is to associate for each user or IoT device multiple addresses for sending and receiving transactions [15]. One relevant piece of research will be to consider privacy by design blockchain based technologies which are already developed in the field of cryptocurrency such as Menero [73] in order to address privacy issues in Internet of Things. So, it should be interesting to take advantage of the state of art in privacy based blockchain and public ledger solutions and adapt them in the field of Internet of Things.

The need to contextualize the environment in which the smart objects and humans evolve is a fundamental approach to address the security in highly distributed and dynamic environments such as IoT. In this paper, we have surveyed basically some recent works (section 7) where most of them exploit the context in order to establish a tradeoff between security and energy consumption. Moreover, other context metrics could be used in order to develop more efficient security solutions. In contrast, Agadakos et al. [2] developed a location-awareness authentication solution for Internet of Things. Their solution exploits the physical presence of a user in some locations to enhance the authentication process without referring to credential keys and passwords that could be compromised by attackers.

Recently, a very promising technology called cloud edge computing has been introduced by Cisco as the convergence between the Internet of Things and cloud computing. The idea behind this concept is to distribute the cloud infrastructure over the edges of users networks, and make it near to final users and IoT devices, which has great benefits in terms of latency and bandwidth and enhances the quality of service and experience of cloud customers [33]. In the future, Internet of Things could take advantage from the edge cloud computing environment in order to meet both performance and security requirements. In this direction, a lot of researches will be devoted to develop efficient security solutions based on edge computing paradigm. A lot of questions are still raised up:

1. How to establish trust between IoT devices and fog nodes in ubiquitous and highly distributed IoT environement ?
2. How to preserve the privacy of IoT devices in cloud edge computing environment where we need to conduct local and real time analysis ? In this direction, Lu et al. [80] proposed fault tolerance and privacy preserving IoT data

Table 8
Comparison of some IoT security solutions.

Solutions \ Challenges		Computation complexity	Communication complexity	Memory	Mobility	Heterogeneity	Scalability	Quality of Service
Confidentiality	Touati et al. [124]	++	–	+	+	+	-	-
	Oualha et al. [99]	+	+	-	+	-	+	+
	Guo et al. [54]	+	-	++	+	+	-	-
	Yao et al. [132]	++	+	+	+	+	-	+
	Su et al. [118]	-	+	+	+	-	-	+
	Thatmann et al. [121]	-	+	+	+	-	+	+
	Chen et al. [29]	++	+	++	-	-	-	+
	Mao et al. [86]	+	+	+	+	+	-	+
Privacy	Evans et al. [47]	+	-	++	+	-	+	+
	Zhang et al. [136]	++	-	++	+	+	-	+
	Alcaide et al. [7]	++	+	+	+	-	+	+
	Huang et al. [63]	+	-	-	+	++	+	+
	Skarmeta et al. [117]	++	+	+	-	-	+	+
	Tonyali et al. [123]	+	-	+	-	-	+	+
Availability	Maleh et al. [84]	+	+	-	+	+	-	-
	Kasinathan et al. [67]	+	-	+	+	+	+	+
	de et al. [37]	-	+	-	+	+	-	+
	Machaka et al. [82]	+	+	-	-	+	-	-
	Shreenivas et al. [109]	+	+	+	+	+	-	-
Blockchain	Hardjono et al. [58]	+	-	+	+	++	++	-
	Gaurav et al. [49]	-	-	-	++	+	++	+
	Hashemi et al. [59]	-	+	-	-	+	++	+
	Kokoris-K et al. [71]	-	+	-	-	+	++	+
	Kamanashis et al. [17]	-	-	-	+	+	++	+
SDN	Flauzac et al. [48]	++	- -	+	-	++	++	-
	Bull et al. [24]	+	-	+	+	+	-	++
	Vandana et al. [126]	+	-	+	-	++	+	+
	Gonzalez et al. [51]	+	-	+	-	+	+	++

We provide in this table a deep analysis and comparison of the solutions we presented previously in this survey according to several security challenges. We use the following notations to assess the level of satisfaction of each solution with respect to the different challenges: + + good; + average; - poor (limited) and - - bad.

aggregation technique in edge computing environment. The proposed scheme is based on homomorphic Paillier encryption, Chinese Remainder Theorem and Oneway hash chain techniques. The aim of this aggregation scheme is to perform statistical operations on IoT data, such as computing means and variances without disclosing the elementary data associated with the different devices nor the identities of those devices.

10. Conclusion

The Internet of things is a new paradigm that comes to revolutionize the world through the connection of various physical objects to the Internet in order to form one unified and intelligent ecosystem. A new intelligent world is emerging nowadays where humans, smart-phones, computers and new intelligent objects are connected to the Internet. In this paper, we surveyed security solutions proposed for Internet of Things' applications. We first categorized the different IoT applications by identifying their security requirements and their inherent challenges. Then we discussed the IoT solutions dealing with confidentiality, privacy and availability which are based on traditional cryptographic solutions. We also reviewed some emerging technologies such as Blockchain and Software Defined Networking which are considered as efficient mechanisms to deal with scalability issues in IoT. Finally, we discussed some security solutions that take care of the context in which IoT applications involve and also the different impacts of security issues on the safety of systems and some countermeasures. Comprehensive comparison of the different approaches was provided based on some criteria, we investigated also some analysis of which techniques are suitable for each kind of IoT application. Despite the efforts that have been spent to deal with the various challenges to which Internet of things face, it's still a lot of open issues to be addressed such as scalability and dynamism issues, especially because Internet of Things is becoming an Internet of Everything where humans, data, processes and objects are evolving together in highly dynamic and complex system.

11. Acknowledgments

This work was carried out and funded in the framework of the Labex MS2T. It was supported by the French Government, through the program "Investments for the future" managed by

the National Agency for Research (Reference ANR-11-IDEX-0004-02).

References

[1] M. M. Abdel-Aziz and A. T. Abdel-Hamid. Hardware low power implementation of attribute-based encryption. In *2016 28th International Conference on Microelectronics (ICM)*, pages 273–276, Dec 2016.

[2] I. Agadakos, P. Hallgren, D. Damopoulos, A. Sabelfeld, and G. Portokalidis. Location-enhanced authentication using the iot: because you cannot be in two places at once. In *Proceedings of the 32nd Annual Conference on Computer Security Applications*, pages 251–264. ACM, 2016.

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4):2347–2376, 2015.

[4] W. AL-mawee. Privacy and security issues in iot healthcare applications for the disabled users a survey. Master's thesis, Western Michigan University, 1903 W Michigan Ave, Kalamazoo, MI 49008, USA, 2012.

[5] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi. Internet of things security: A survey. *Journal of Network and Computer Applications*, 2017.

[6] S. Alanazi, J. Al-Muhtadi, A. Derhab, K. Saleem, A. N. AlRomi, H. S. Alholaibah, and J. J. Rodrigues. On resilience of wireless mesh routing protocol against dos attacks in iot-based ambient assisted living applications. In *17th International Conference on E-health Networking, Application & Services (HealthCom)*, pages 205–210. IEEE, 2015.

[7] A. Alcaide, E. Palomar, J. Montero-Castillo, and A. Ribagorda. Anonymous authentication for privacy-preserving iot target-driven applications. *Computers & Security*, 37:111–123, 2013.

[8] M. Ali, J. C. Nelson, R. Shea, and M. J. Freedman. Blockstack: A global naming and storage system secured by blockchains. In *USENIX Annual Technical Conference*, pages 181–194, 2016.

[9] M. Ambrosin, M. Conti, and T. Dargahi. On the feasibility of attribute-based encryption on smartphone devices. In *Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems*, pages 49–54. ACM, 2015.

[10] M. Atzori. Blockchain-based architectures for the internet of things: A survey. *Available at SSRN: https://ssrn.com/abstract=2846810*, January 2017.

[11] L. Axon. Privacy-awareness in blockchain-based pki. 2015.

[12] A. Aydeger, N. Saputro, K. Akkaya, and M. Rahman. Mitigating crossfire attacks using sdn-based moving target defense. In *2016 IEEE 41st Conference on Local Computer Networks (LCN)*, pages 627–630, Nov 2016.

[13] A. Bahga and V. K. Madisetti. Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications*, 9(10):533, 2016.

[14] A. Balte, A. Kashid, and B. Patil. Security issues in internet of things (iot): A survey. *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(4), 2015.

[15] S. Barber, X. Boyen, E. Shi, and E. Uzun. Bitter to better—how to make bitcoin a better currency. In *International Conference on Financial Cryptography and Data Security*, pages 399–414. Springer, 2012.

[16] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy, 2007. SP'07*, pages 321–334. IEEE, 2007.

[17] K. Biswas and V. Muthukkumarasamy. Securing smart cities using blockchain technology. In *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pages 1392–1393. IEEE, Dec 2016.

[18] R. Blom. An optimal class of symmetric key generation systems. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 335–338. Springer, 1984.

[19] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In *Annual International Cryptology Conference*, pages 213–229. Springer, 2001.

[20] S. Brief. Sdn security considerations in the data center, 2013.

[21] P. J. Bruening and K. K. Waterman. Data tagging for new information governance models. *IEEE Security Privacy*, 8(5):64–68, Sept 2010.

[22] J. Brunel, D. Chemouil, L. Rioux, M. Bakkali, and F. Vallée. A viewpoint-based approach for formal safety & security assessment of system architectures. In *11th Workshop on Model-Driven Engineering, Verification and Validation*, volume 1235, pages 39–48, 2014.

[23] J. Brygier and M. Oezer. Safety and security for the internet of things. In *8th European Congress on Embedded Real Time Software and Systems (ERTS 2016)*, 2016.

[24] P. Bull, R. Austin, E. Popov, M. Sharma, and R. Watson. Flow based security for iot devices using an sdn gateway. In *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Future Internet of Things and Cloud (FiCloud),*, pages 157–163. IEEE, July 2016.

[25] I. Butun, S. D. Morgera, and R. Sankar. A survey of intrusion detection systems in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 16(1):266–282, 2014.

[26] A. A. Cardenas, S. Amin, and S. Sastry. Secure control: Towards survivable cyber-physical systems. In *2008. ICDCS'08. 28th International Conference on Distributed Computing Systems Workshops*, pages 495–500. IEEE, 2008.

[27] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *Proceedings. 2003 Symposium on Security and Privacy, 2003*, pages 197–213. IEEE, 2003.

[28] I. Chatzigiannakis, A. Pyrgelis, P. G. Spirakis, and Y. C. Stamatiou. Elliptic curve based zero knowledge proofs and their applicability on resource constrained devices. In *2011 IEEE 8th International Conference on Mobile Adhoc and Sensor Systems (MASS)*, pages 715–720. IEEE, 2011.

[29] W. Chen. An ibe-based security scheme on internet of things. In *Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on*, volume 3, pages 1046–1049. IEEE, 2012.

[30] T. Choi, H. B. Acharya, and M. G. Gouda. The best keying protocol for sensor networks. *Pervasive and Mobile Computing*, 9(4):564–571, 2013.

[31] K. Christidis and M. Devetsikiotis. Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:2292–2303, 2016.

[32] C. Cocks. An identity based encryption scheme based on quadratic residues. In *IMA International Conference on Cryptography and Coding*, pages 360–363. Springer, 2001.

[33] F. Computing. the internet of things: Extend the cloud to where the things are, 2016.

[34] M. Conoscenti, A. Vetrò, and J. C. De Martin. Blockchain for the internet of things: a systematic literature review. pages 1–6, November 2016.

[35] B. Cusack, Z. Tian, and A. K. Kyaw. Identifying dos and ddos attack origin: Ip traceback methods comparison and evaluation for iot. In *International Conference on Interoperability in IoT*, pages 127–138. Springer, 2016.

[36] F. Dalipi and S. Y. Yayilgan. Security and privacy considerations for iot application on smart grids: Survey and research challenges. In *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pages 63–68. IEEE, Aug 2016.

[37] F. M. de Almeida, A. de RL Ribeiro, E. D. Moreno, and C. A. Montesco. Performance evaluation of an artificial neural network multilayer perceptron with limited weights for detecting denial of service attack on internet of things. *training*, 11:12.

[38] A. Di Mauro, X. Fafoutis, and N. Dragoni. Adaptive security in odmac for multihop energy harvesting wireless sensor networks. *International Journal of Distributed Sensor Networks*, 11(4):760302, 2015.

[39] R. Di Pietro, L. V. Mancini, and S. Jajodia. Providing secrecy in key management protocols for large wireless sensors networks. *Ad Hoc Networks*, 1(4):455–468, 2003.

[40] G. Dini and L. Lopriore. Key propagation in wireless sensor networks. *Computers & Electrical Engineering*, 41:426–433, 2015.

[41] M. Donohoe, B. Jennings, and S. Balasubramaniam. Context-awareness and the smart grid: Requirements and challenges. *Computer Networks*, 79:263–282, 2015.

[42] W. Du, J. Deng, Y. S. Han, and P. K. Varshney. A key predistribution scheme for sensor networks using deployment knowledge. *IEEE Trans-*

actions on dependable and secure computing, 3(1):62–77, 2006.

[43] D. R. Duran, E. Robinson, A. J. Kornecki, and J. Zalewski. Safety analysis of autonomous ground vehicle optical systems: Bayesian belief networks approach. In *2013 Federated Conference on Computer Science and Information Systems (FedCSIS)*, pages 1419–1425. IEEE, 2013.

[44] D. P. Eames and J. Moffett. The integration of safety and security requirements. In *International Conference on Computer Safety, Reliability, and Security*, pages 468–480. Springer, 1999.

[45] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM conference on Computer and communications security*, pages 41–47. ACM, 2002.

[46] D. Evans. The Internet of Things how the next evolution of the internet is changing everything. Technical report, 04 2011.

[47] D. Evans and D. M. Eyers. Efficient data tagging for managing privacy in the internet of things. In *2012 IEEE International Conference on Green Computing and Communications (GreenCom)*, pages 244–248. IEEE, 2012.

[48] O. Flauzac, C. González, A. Hachani, and F. Nolot. Sdn based architecture for iot and improvement of the security. In *2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops*, pages 688–693. IEEE, March 2015.

[49] K. Gaurav, P. Goyal, V. Agrawal, and S. L. Rao. Iot transaction security. In *5th International Conference on the Internet of Things (IoT)*, Seoul, S. Korea, october 2015.

[50] M. Gerla, E. K. Lee, G. Pau, and U. Lee. Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. In *2014 IEEE World Forum on Internet of Things (WF-IoT)*, pages 241–246. IEEE, March 2014.

[51] C. Gonzalez, S. M. Charfadine, O. Flauzac, and F. Nolot. Sdn-based security framework for the iot in distributed grid. In *2016 International Multidisciplinary Conference on Computer and Energy Science (SpliTech)*, pages 1–5. IEEE, July 2016.

[52] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 89–98. Acm, 2006.

[53] J. Granjal, E. Monteiro, and J. S. Silva. Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials*, 17(3):1294–1312, 2015.

[54] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan. Cp-abe with constant-size keys for lightweight devices. *IEEE transactions on information forensics and security*, 9(5):763–771, 2014.

[55] J. Guo, R. Chen, and J. J. Tsai. A survey of trust computation models for service management in internet of things systems. *Computer Communications*, 97:1–14, 2017.

[56] S. Gusmeroli, S. Piccione, and D. Rotondi. A capability-based security approach to manage access control in the internet of things. *Mathematical and Computer Modelling*, 58(5):1189–1205, 2013.

[57] M. Hamdi and H. Abie. Game-based adaptive security in the internet of things for ehealth. In *2014 IEEE International Conference on Communications (ICC)*, pages 920–925. IEEE, June 2014.

[58] T. Hardjono and N. Smith. Cloud-based commissioning of constrained devices using permissioned blockchains. In *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*, pages 29–36. ACM, 2016.

[59] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell. World of empowered iot users. In *2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pages 13–24. IEEE, April 2016.

[60] D. He, J. Bu, S. Zhu, S. Chan, and C. Chen. Distributed access control with privacy support in wireless sensor networks. *IEEE Transactions on Wireless Communications*, 10(10):3472–3481, 2011.

[61] H. Hellaoui, A. Bouabdallah, and M. Koudil. Tas-iot: Trust-based adaptive security in the iot. In *2016 IEEE 41st Conference on Local Computer Networks (LCN)*, pages 599–602. IEEE, 2016.

[62] P. Hu. A system architecture for software-defined industrial internet of things. In *2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB)*, pages 1–5. IEEE, Oct 2015.

[63] X. Huang, R. Fu, B. Chen, T. Zhang, and A. Roscoe. User interactive internet of things privacy preserved access control. In *2012 International Conference for Internet Technology And Secured Transactions*, pages 597–602. IEEE, 2012.

[64] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle. 6lowpan fragmentation attacks and mitigation mechanisms. In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, pages 55–66. ACM, 2013.

[65] W. Huo-wang and Z. Cheng. Parallel clustering-based k-anonymity algorithm in internet of things. *Information Technology*, 12:003, 2013.

[66] R. S. M. Joshitta and Arockiam. Security in iot environment: A survey. *Int. Journal of Information Technology & Mechanical Engineering-IJITME*, 2(7):1–8, 2016.

[67] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits. Denial-of-service detection in 6lowpan based internet of things. In *2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 600–607. IEEE, 2013.

[68] B. Khelifa and S. Abla. Security concerns in smart grids: Threats, vulnerabilities and countermeasures. In *2015 3rd International Renewable and Sustainable Energy Conference (IRSEC)*, pages 1–6. IEEE, Dec 2015.

[69] H. M. Kim and M. Laskowski. Towards an ontology-driven blockchain design for supply chain provenance. 2016.

[70] B. Klugah-Brown, J. B. A. Kanpogninge, and X. Qi. A signcryption scheme from certificateless to identity-based environment for wsns into iot. *International Journal of Computer Applications*, 120(9), 2015.

[71] L. Kokoris-Kogias, L. Gasser, I. Khoffi, P. Jovanovic, N. Gailly, and B. Ford. Managing identities using blockchains and cosi. In *9th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2016)*, number EPFL-TALK-220210, 2016.

[72] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand. A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering & System Safety*, 139:156–178, 2015.

[73] A. Kumar, C. Fischer, S. Tople, and P. Saxena. A traceability analysis of monero's blockchain. *IACR Cryptology ePrint Archive*, 2017:338, 2017.

[74] J. S. Kumar and D. R. Patel. A survey on internet of things: Security and privacy issues. *International Journal of Computer Applications*, 90(11), 2014.

[75] Y. Lee, W. Lee, G. Shin, and K. Kim. Assessing the impact of dos attacks on iot gateway. Bangkok, Thailand, December 2016.

[76] Y. Leng and L. Zhao. Novel design of intelligent internet-of-vehicles management system based on cloud-computing and internet-of-things. In *Proceedings of 2011 International Conference on Electronic Mechanical Engineering and Information Technology*, volume 6, pages 3190–3193. IEEE, Aug 2011.

[77] F. Li, Y. Han, and C. Jin. Practical access control for sensor networks in the context of the internet of things. *Computer Communications*, 89:154–164, 2016.

[78] J. Liu, Y. Xiao, S. Li, W. Liang, and C. P. Chen. Cyber security and privacy issues in smart grids. *IEEE Communications Surveys & Tutorials*, 14(4):981–997, 2012.

[79] A. Loibl. Namecoin. *namecoin. info*, 2014.

[80] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani. A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced iot. *IEEE Access*, 5:3302–3312, 2017.

[81] C. Ma, K. Xue, and P. Hong. Distributed access control with adaptive privacy preserving property for wireless sensor networks. *Security and Communication Networks*, 7(4):759–773, 2014.

[82] P. Machaka, A. McDonald, F. Nelwamondo, and A. Bagula. Using the cumulative sum algorithm against distributed denial of service attacks in internet of things. In *International Conference on Context-Aware Systems and Applications*, pages 62–72. Springer, 2015.

[83] M. Mainelli and C. von Gunten. Chain of a lifetime: How blockchain technology might transform personal insurance. *Long Finance*, 2014.

[84] Y. Maleh, E. Abdellah, and M. Belaissaoui. Dos attacks analysis and improvement in dtls protocol for internet of things. In ACM, editor, *ACM International conference on Big Data and Advanced Wireless technologies (BDAW'2016)*, Nov. 2016.

[85] L. Malina, J. Hajny, R. Fujdiak, and J. Hosek. On perspective of security and privacy-preserving solutions in the internet of things. *Computer Networks*, 102:83 – 95, 2016.

[86] Y. Mao, J. Li, M.-R. Chen, J. Liu, C. Xie, and Y. Zhan. Fully secure fuzzy identity-based encryption for secure iot communications. *Computer Standards & Interfaces*, 44:117–121, 2016.

[87] M. N. Mejri, J. Ben-Othman, and M. Hamdi. Survey on vanet security challenges and possible cryptographic solutions. *Vehicular Communications*, 1(2):53–66, 2014.

[88] B. Miller and D. Rowe. A survey scada of and critical infrastructure incidents. In *Proceedings of the 1st Annual conference on Research in information technology*, pages 51–56. ACM, 2012.

[89] R. Mitchell and I.-R. Chen. A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys (CSUR)*, 46(4):55, 2014.

[90] R. Mitchell and R. Chen. Effect of intrusion detection and response on reliability of cyber physical systems. *IEEE Transactions on Reliability*, 62(1):199–210, 2013.

[91] Y. Mo and B. Sinopoli. Secure control against replay attacks. In *2009. Allerton 2009. 47th Annual Allerton Conference on Communication, Control, and Computing*, pages 911–918. IEEE, 2009.

[92] S. Müller, S. Katzenbeisser, and C. Eckert. Distributed attribute-based encryption. In *International Conference on Information Security and Cryptology-ICISC 2008*, volume 5461, pages 20–36, Berlin, Heidelberg, 2009. Springer, Springer Berlin Heidelberg.

[93] R. Neisse, G. Steri, G. Baldini, E. Tragos, I. N. Fovino, and M. Botterman. Dynamic context-aware scalable and trust-based iot security, privacy framework. *Chapter in Internet of Things Applications-From Research and Innovation to Market Deployment, IERC Cluster Book*, 2014.

[94] K. T. Nguyen, M. Laurent, and N. Oualha. Survey on secure communication protocols for the internet of things. *Ad Hoc Networks*, 32:17–31, 2015.

[95] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li. Achieving k-anonymity in privacy-aware location-based services. In *INFOCOM, 2014 Proceedings IEEE*, pages 754–762. IEEE, 2014.

[96] H. Noura. *Adaptation of Cryptographic Algorithms According to the Applications Requirements and Limitations : Design, Analyze and Lessons Learned*. HDR dissertation, UNIVERSITY of PIERRE MARIE CURIE -Paris VI, 2016.

[97] F. Olivier, G. Carlos, and N. Florent. Sdn based architecture for clustered wsn. In *2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pages 342–347. IEEE, July 2015.

[98] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman. Access control in the internet of things: Big challenges and new opportunities. *Computer Networks*, 112:237 – 262, 2017.

[99] N. Oualha and K. T. Nguyen. Lightweight attribute-based encryption for the internet of things. In *2016 25th International Conference on Computer Communication and Networks (ICCCN)*, pages 1–6. IEEE, 2016.

[100] C. Raspotnig, P. Karpati, and V. Katta. A combined process for elicitation and analysis of safety and security requirements. In *Enterprise, business-process and information systems modeling*, pages 347–361. Springer, 2012.

[101] A. Rghioui, A. Khannous, and M. Bouhorma. Denial-of-service attacks on 6lowpan-rpl networks: Threats and an intrusion detection system proposition. *Journal of Advanced Computer Science & Technology*, 3(2):143, 2014.

[102] A. Rizzardi, D. Miorandi, S. Sicari, C. Cappiello, and A. Coen-Porisini. Networked smart objects: moving data processing closer to the source. In *Internet of Things. IoT Infrastructures: Second International Summit, IoT 360 2015, Rome, Italy, October 27-29, 2015, Revised Selected Papers, Part II*, pages 28–35. Springer, 2016.

[103] S. S. N. Roby. Application of blockchain technology in online voting. 2017.

[104] R. Roman, J. Zhou, and J. Lopez. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10):2266 – 2279, 2013. Towards a Science of Cyber SecuritySecurity and Identity Architecture for the Future Internet.

[105] A.-R. Sadeghi, C. Wachsmann, and M. Waidner. Security and privacy challenges in industrial internet of things. In *2015 52nd ACM/EDAC/IEEE on Design Automation Conference (DAC)*, pages 1–6. IEEE, June 2015.

[106] A. Sahai and B. Waters. Fuzzy identity-based encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 457–473. Springer, 2005.

[107] S. Sahraoui and A. Bilami. Efficient hip-based approach to ensure lightweight end-to-end security in the internet of things. *Computer Networks*, 91:26 – 45, 2015.

[108] P. G. Shah and J. Ambareen. A survey of security challenges in internet of things (iot) integration with wsn. *AUSJOURNAL*, 2014.

[109] D. Shreenivas, S. Raza, and T. Voigt. Intrusion detection in the rpl-connected 6lowpan networks. In *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security*, pages 31–38. ACM, 2017.

[110] S. Sicari, A. Rizzardi, L. Grieco, G. Piro, and A. Coen-Porisini. A policy enforcement framework for internet of things applications in the smart health. *Smart Health*, 2017.

[111] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini. Security, privacy and trust in internet of things: The road ahead. *Computer Networks*, 76:146–164, 2015.

[112] S. Sicari, A. Rizzardi, D. Miorandi, C. Cappiello, and A. Coen-Porisini. A secure and quality-aware prototypical architecture for the internet of things. *Information Systems*, 58:43–55, 2016.

[113] S. Sicari, A. Rizzardi, D. Miorandi, C. Cappiello, and A. Coen-Porisini. Security policy enforcement for networked smart objects. *Computer Networks*, 108:133–147, 2016.

[114] S. Sicari, A. Rizzardi, D. Miorandi, and A. Coen-Porisini. Internet of things: Security in the keys. In *Q2SWinet MSWiM*, pages 129–133, 2016.

[115] I. Silva, R. Leandro, D. Macedo, and L. A. Guedes. A dependability evaluation tool for the internet of things. *Computers & Electrical Engineering*, 39(7):2005–2018, 2013.

[116] G. Sindre. A look at misuse cases for safety concerns. In *Situational Method Engineering: Fundamentals and Experiences*, pages 252–266. Springer, 2007.

[117] A. F. Skarmeta, J. L. Hernandez-Ramos, and M. V. Moreno. A decentralized approach for security and privacy challenges in the internet of things. In *2014 IEEE World Forum on Internet of Things (WF-IoT)*, pages 67–72. IEEE, 2014.

[118] J. Su, D. Cao, B. Zhao, X. Wang, and I. You. epass: An expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the internet of things. *Future Generation Computer Systems*, 33:11 – 18, 2014. Special Section on Applications of Intelligent Data and Knowledge Processing Technologies; Guest Editor: Dominik Ślęzak.

[119] L. Sweeney. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):557–570, 2002.

[120] A. V. Taddeo, M. Mura, and A. Ferrante. Qos and security in energy-harvesting wireless sensor networks. In *Proceedings of 2010 International Conference on Security and Cryptography (SECRYPT)*, pages 1–10. IEEE, 2010.

[121] D. Thatmann, S. Zickau, A. Förster, and A. Küpper. Applying attribute-based encryption on publish subscribe messaging patterns for the internet of things. In *2015 IEEE International Conference on Data Science and Data Intensive Systems (DSDIS)*, pages 556–563. IEEE, 2015.

[122] M. Tilal and R. Minhas. Effects of jamming on ieee 802.11 p systems. Master's thesis, Chalmers University of Technology, Göteborg, Sweden, November 2010.

[123] S. Tonyali, O. Cakmak, K. Akkaya, M. M. Mahmoud, and I. Guvenc. Secure data obfuscation scheme to enable privacy-preserving state estimation in smart grid ami networks. *IEEE Internet of Things Journal*, 3(5):709–719, 2016.

[124] L. Touati, Y. Challal, and A. Bouabdallah. C-cp-abe: Cooperative ciphertext policy attribute-based encryption for the internet of things. In *2014 International Conference on Advanced Networking Distributed Systems and Applications (INDS)*, pages 64–69. IEEE, 2014.

[125] L. Valenta and B. Rowan. Blindcoin: Blinded, accountable mixes for bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 112–126. Springer, 2015.

[126] C. Vandana. Security improvement in iot based on software defined networking (sdn). *International Journal of Engineering and Technology Research (IJSETR)*, 5(1):291–295, january 2016.

[127] B. Vikas. Internet of things (iot): A survey on privacy issues and security. *International Journal of Scientific Research in Science, Engineering and Technology*, 1(3):168–173, May 2015.

[128] E. K. Wang, T.-Y. Wu, C.-M. Chen, Y. Ye, Z. Zhang, and F. Zou. Mdpas: Markov decision process based adaptive security for sensors in internet of things. In *Genetic and Evolutionary Computing*, pages 389–397. Springer, 2015.

[129] Z. Wang, H. Ding, J. Han, and J. Zhao. Secure and efficient control transfer for iot devices. *International Journal of Distributed Sensor Networks*, 9(11):503404, january 2013.

[130] S. Wilkinson, T. Boshevski, J. Brandoff, and V. Buterin. Storj a peer-to-peer cloud storage network. 2014.

[131] Z. Yan, P. Zhang, and A. V. Vasilakos. A survey on trust management for internet of things. *Journal of network and computer applications*, 42:120–134, 2014.

[132] X. Yao, Z. Chen, and Y. Tian. A lightweight attribute-based encryption scheme for the internet of things. *Future Generation Computer Systems*, 49:104 – 112, 2015.

[133] S. Yu, K. Ren, and W. Lou. Fdac: Toward fine-grained distributed data access control in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 22(4):673–686, April 2011.

[134] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems*, 40(10):218, 2016.

[135] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. Internet of things for smart cities. *IEEE Internet of Things Journal*, 1(1):22–32, Feb 2014.

[136] R. Zhang, Y. Zhang, and K. Ren. Distributed privacy-preserving access control in sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 23(8):1427–1438, Aug 2012.

[137] K. Zhao and L. Ge. A survey on the internet of things security. In *2013 9th International Conference on Computational Intelligence and Security (CIS)*, pages 663–667. IEEE, Dec 2013.

[138] S. Zhu, S. Setia, and S. Jajodia. Leap+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Trans. Sen. Netw.*, 2(4):500–528, Nov. 2006.