Evaluating Critical Security Issues of the IoT World: Present and Future Challenges

Mario Frustaci, Pasquale Pace, *Member, IEEE*, Gianluca Aloi, *Member, IEEE*,
and Giancarlo Fortino, *Senior Member, IEEE*

***Abstract*—Social Internet of Things (SIoT) is a new paradigm where Internet of Things (IoT) merges with social networks, allowing people and devices to interact, and facilitating information sharing. However, security and privacy issues are a great challenge for IoT but they are also enabling factors to create a "trust ecosystem." In fact, the intrinsic vulnerabilities of IoT devices, with limited resources and heterogeneous technologies, together with the lack of specifically designed IoT standards, represent a fertile ground for the expansion of specific cyber threats. In this paper, we try to bring order on the IoT security panorama providing a taxonomic analysis from the perspective of the three main key layers of the IoT system model: 1) perception; 2) transportation; and 3) application levels. As a result of the analysis, we will highlight the most critical issues with the aim of guiding future research directions.**

***Index Terms*—Cyber threats, Internet of Things (IoT), IoT protocols, IoT security, IoT system model, trust.**

I. Introduction

In THE next future, the Internet of Things (IoT) paradigm will involve billion of smart-devices with processing, sensing and actuating capabilities able to be connected to the Internet [1], [2]. Integrating social networking concepts into the IoT has led to the Social IoT (SIoT) concept which enables people and connected devices to interact, facilitating information sharing [3]. However, interoperability [4], security, and privacy issues are a great challenge for IoT but they are also enabling factors to create a "trust and interoperable ecosystem." In fact, not solving these issues, the SIoT paradigm will not reach enough popularity and all its potential can be lost.

Security issue is emphasized by the lack of standards specifically designed for devices with limited resources and heterogeneous technologies. In addition, these devices, due to many vulnerabilities, represent a "fertile ground" for existing cyber threats. In fact, at the end of 2016, there were distributed denial of service (DDoS) attacks to the DNS provider Dyn (which support major Internet platforms and services such as PayPal, Twitter, VISA, etc.) through a botnet consisting of a large number of vulnerable IoT devices (such as printers, IP cameras, residential gateways, and baby monitors) that had been infected by the Mirai malware. With an estimated load of 1.2 terabits per second, the attack is, according to experts, the largest DDoS on record [5]. In addition, in the same period, researchers uncovered a flaw in the radio protocol ZigBee [6] that has been shown and demonstrated by using an aerial drone to target a set of smart Philips light bulbs in an office tower, infecting the bulbs with a virus that let the attackers to turn the lights on and off flashing an "SOS" message in Morse code; moreover, this malware was also able to spread like a pathogen among the devices neighbors.

Finally, another matter of concern for IoT, is the privacy in the protection of the personal data collected by such IoT systems since it is necessary to provide full awareness and control of the automatic data flow to the generic end user.

Starting from this worrying and challenging context, this paper discusses the current status and how to design IoT security. In Section II, we discuss about a generic model for IoT Systems with specific reference to threats. In Section III, we define the concept of trust and its importance in IoT to create social relationships between unknown entities. In Section IV, we define how security must be correctly designed to support the IoT paradigm by exhibiting some generic policies and strategies which should be redesigned to address specific characteristics of IoT world (i.e., limited resources and technological heterogeneity). A key step to include security in IoT Systems is also related to the secure communication protocols used in a way that data in transit are confidential, reliable, and available by preventing cyber attacks. In fact, in Section V we analyze some widely used IoT protocols dealing with security issues and describing innovative solutions presented in the scientific literature. Finally, in Section VI we discuss where it should be directed the scientific research in the near future to solve the most serious security IoT issues.

II. Threats in IoT System Model

A generic IoT system can be fully represented and described by using three main key layers: 1) *perception*; 2) *transportation*; and 3) *application*. Each of these system levels summarized in Fig. 1 has its own specific technologies that bring issues and some possible security weaknesses. In fact,

Manuscript received July 15, 2017; revised September 27, 2017; accepted October 17, 2017. Date of publication October 27, 2017; date of current version August 9, 2018. This work was supported by the European Union under the framework of INTER-IoT Research and Innovation action - Horizon 2020 European Project, Grant Agreement 687283. *(Corresponding author: Pasquale Pace.)*

The authors are with the Department of Informatics, Modeling, Electronics and System Engineering, University of Calabria, 87036 Rende, Italy (e-mail: m.frustaci@dimes.unical.it; ppace@dimes.unical.it; aloi@dimes.unical.it; fortino@dimes.unical.it).

Digital Object Identifier 10.1109/JIOT.2017.2767291

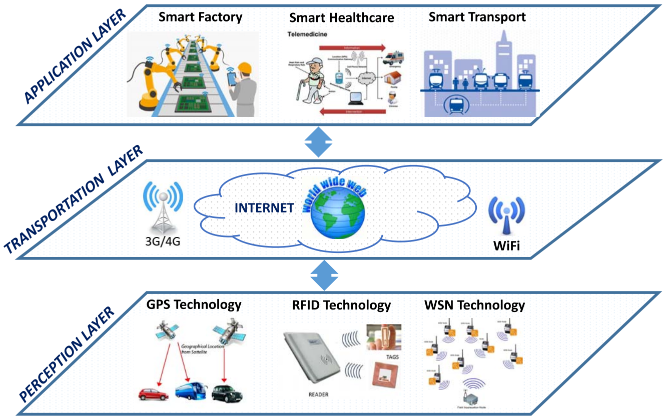

Fig. 1. IoT system model.

in [7] the security problems of each layer are analyzed separately by looking for new robust and feasible solutions.

A. Perception Layer

The first layer is related to the physical IoT sensors to support data collection and processing on different common technologies such as radio-frequency identification (RFID), wireless sensor network (WSN), RFID sensor network (RSN), and GPS. This layer includes sensors and actuators to perform different measurements (i.e., temperature, acceleration, humidity, etc.) and functionalities such as querying location [8]. Due to the limited node resources and distributed organized structure, the main security threats coming from the perception layer are as follows.

1) *Physical Attacks:* These kinds of attacks are focused on the hardware components of the IoT system and the attacker needs to be physically close or into the IoT system in order to make the attacks working. Some examples of these attacks are as follows.
   a) *Node Tampering:* The attacker can cause damage to a sensor node, by physically replacing the entire node or part of its hardware or even electronically interrogating the nodes to gain access and alter sensitive information, such as shared cryptographic keys or routing tables.
   b) *Malicious Code Injection:* The attacker compromises a node by physically injecting it with malicious code that would give him access to the IoT system.
2) *Impersonation:* Authentication in the distributed environment is very difficult, allowing malicious nodes to use a fake identity for malicious or collusion attacks
3) *Denial of Service (DoS) Attacks:* Attackers exploit the finite processing ability of the nodes, making them unavailable.
4) *Routing Attacks:* Intermediate malicious nodes (e.g., in a WSN) might modify the right routing paths during the data collection and forwarding process.
5) *Data Transit Attacks:* Various attacks on the confidentiality and integrity during data transit [e.g., sniffing and man-in-the-middle (MITM)].

B. Transportation Layer

Transportation layer mainly provides ubiquitous access environment for the perception layer. The purpose of this layer is to transmit the gathered information, received from the perception layer, to any particular information processing system through existing communication networks used by both access networks (3G, WiFi, ad hoc network, etc.) or core networks (Internet).

In [9], there is a brief overview of security issues in wireless networks such as cellular networks. According to this paper, the open and heterogeneous architecture of an IP-based LTE network, is resulting in increasing number of security threats compared to the 3G networks.

Generally, at this level, the main security threats are as follows.

1) *Routing Attacks:* Intermediate malicious nodes (e.g., in a WSN) might modify the right routing paths during the data collection and forwarding process.
2) *DoS Attacks:* Because of the heterogeneity and complexity of IoT network, the transportation layer is vulnerable to get attacked.
3) *Data Transit Attacks:* Various attacks on the confidentiality and integrity during data transit in access or core networks.

C. Application Layer

The application layer provides the services requested by customers. For instance, the application layer can provide temperature and air humidity measurements to the customers asking for such data. The importance of this layer for the IoT is that it has the ability to provide high-quality smart services to meet customers' needs. Many different IoT environments (i.e., smart city, smart healthcare, and smart factory) can be implemented within this level; moreover, an application support sublayer, to support all sorts of business services and to realize intelligent computation and resources allocation, could be implemented throughout specific middleware and cloud computing platforms.

The main security threats within this layer are as follows.

1) *Data Leakage:* The attacker can easily steal data (also data user, e.g., user password) by knowing vulnerabilities of the service or application.
2) *DoS Attack:* Attackers can destroy the availability of the application or service itself.
3) *Malicious Code Injection*: Attackers can upload malicious codes in software applications exploiting the known vulnerabilities.

III. Trust in the IoT World

Trust management has been proven to be a useful technology for providing security service and, as a consequence, has been used in many applications such as collaborative Web-based platforms [10], social media [11], semantic Web [12], or online shopping [13].

For the IoT world, the development of trust mechanisms is fundamental to help people to overcome perceptions of

TABLE I
THREATS IN IoT SYSTEM MODEL

Layer	Main Threats
Application Level	Data Leakage
	DoS Attacks
	Malicious Code Injection
Transportation Level	Routing Attacks
	DoS Attacks
	Data Transit Attacks
Perception Level	Physical Attacks
	Impersonation
	DoS Attacks
	Routing Attacks (e.g. in WSN, RSN)
	Data Transit Attacks (in WSN or RSN)

uncertainty and risk in using IoT services and applications [14], [15], [19]. Especially, in SIoT, trust plays a key role in establishing trustworthy social relationships between unknown entities. In fact, in this context, IoT devices mimic autonomously the social behavior of their human counterparts according to the owners' social networks and build up social relationships with other trust devices in order to provide services to the humans.

A. Trust Properties

Trust is a very complicated concept that is influenced by many measurable and nonmeasurable properties. It is strictly related to security since ensuring system security and user safety is a necessity to gain trust. However, trust is more than security. Another important concept related to trust is privacy that is the ability of an entity to determine whether, when, and to whom information about itself is to be released or disclosed.

The properties influencing a trust decision can be classified into five categories [16].

1) Trustee's objective properties, such as a trustee's security, dependability (reliability, maintainability, usability, and safety) and privacy preservation.
2) Trustee's subjective properties, such as trustee honesty, benevolence and goodness.
3) Trustor's subjective properties, such as trustor disposition and willingness to trust.
4) Trustor's objective properties, such as the criteria or policies specified by the trustor for a trust decision.
5) *Context:* The situation or environment (time, place, and involved entities) in which the entities operate. Trust is different depending on the context: the trust relationships of a IoT device in a controlled environment are different from those a public space where there are unknown and untrusted entities.

B. Importance of Trust

The main advantages of introducing trust mechanism into IoT are as follows [17].

1) *Certainty in Collaboration:* Uncertainty is originated basically from two sources: a) information asymmetry (a partner does not have all the information it needs about others) and b) opportunism (transacting partners have different goals).
2) *Excellent Flexibility:* Trust mechanisms can deal with changeable security condition and personalized security request. Users or nodes can define personalized policies to evaluate whether an object is trusted or not. Every participant can define one or multiple policies to perform decision-making according to their request.
3) *Better Efficiency:* Trust management systems must be lightweight enough to provide a good performance taking into account energy constrains of several sensor nodes. For example, for the routing process, sensor nodes might need to know which other nodes to trust when forwarding a packet, so as to choose whether to send the information either through the fastest link or through the nodes that have spent less energy. Furthermore, the bandwidth can be evaluated by trust value so as to select routing properly to balance the load.
4) *Uniforming Decision-Making for Heterogeneous IoT:* Trust can be supported across multiple IoT domains based on trust chain technology.
5) *Compatibility Between Trust and Security:* In fact, a trust management system can assist and/or take advantage of other security protocols and mechanisms [e.g., key management, intrusion detection system (IDS), and privacy]. For example, regarding the key management systems, a node can use the trust measurements to revoke the keys of an untrusted entity. In this regard, the work in [18] proposes an adaptive trust management protocol for SIoT systems to enhance the security against malicious attacks.

C. Trust Management Goals

To provide trustworthy IoT system, trust management in IoT should achieve the following objectives grouped in different categories [16].

1) *Layer Goals:*
   a) *Data Perception Trust:* Data sensing and collection should be reliable in IoT (*perception layer goal*).
   b) *Data Communication Trust:* Data should be securely transmitted in the IoT systems (*perception and transportation layer goal*).
   c) *Data Fusion and Mining Trust:* Data collected in IoT should be processed and analyzed in a trustworthy way, e.g., with regard to privacy preservation and accuracy (*application layer goal*).
   d) *Quality of IoT Services:* This objective should be ensured through "only here, only me and only now" services (*application layer goal*).
   e) *Human–Computer Trust Interaction:* To support user usability using IoT services (*application layer goal*).
2) *Cross-Layer Goals:*
   a) *Generality:* Trust management for various IoT systems and services should be generic in order to be widely applied.

b) *Trust Relationship and Decision:* It is necessary a Trust relationship evaluation for all IoT entities in order to make the best decision for intelligent and autonomic trust management.

c) *System Security and Robustness:* System security and dependability are fundamentals to gain user confidence.

d) *Privacy Preservation:* User privacy must be preserved according to user policy.

e) *Identity Trust:* Entities identities should be well managed in a trustworthy way considering the objective properties of IoT system (e.g., identity privacy) and subjective properties of IoT entities (e.g., user belief) and context that may influence identity management policies.

Only addressing these goals, it is possible to achieve a comprehensive and holistic trust management for IoT.

IV. IoT Security

Security in IoT devices is often neglected or treated as an afterthought from the IoT manufacturers. This is mostly due to the short time to market and costs reduction driving the device's design and development process. The few devices that support some protection usually employ software level solutions, such as firmware signing. However, focusing the attention on the software-based protection schemes often leaves the hardware unintentionally vulnerable (e.g., debug interfaces open), allowing for new attacks; as a reference example, the work in [20] clearly demonstrated that a nonsecure hardware platform will inevitably lead to a nonsecure software stack.

In this section, we discuss about the design of security techniques for IoT systems and devices also highlighting the differences with traditional IT security. In addition, we provide useful policies to secure IoT systems from some standard threats summarized in Table I.

A. Security Goals: CIA Security Model

The security triad, a distinguished model for the development of security mechanisms, implements the security by making use of three main areas which are: data confidentiality, integrity, and availability (CIA security model, shown in Fig. 2).

Data confidentiality is the ability to provide confidence to user about the privacy of the sensitive information by using different mechanisms so that its disclosure to the unauthorized party is prevented and can be accessed by the authorized users only. Data confidentiality is usually supported through different mechanisms such as data encryption or access control.

Data integrity refers to the protection of useful information from the cybercriminals or the external interference during data transit or rest through some common methods like data integrity algorithms preventing data alteration.

Data availability ensures the immediate access of authorized party to their information resources not only in the normal conditions but also in disastrous conditions. The attacks on the services like DoS attack can deny data availability. The most famous mechanisms to protect availability are: firewall, IDS, and redundancy methods.

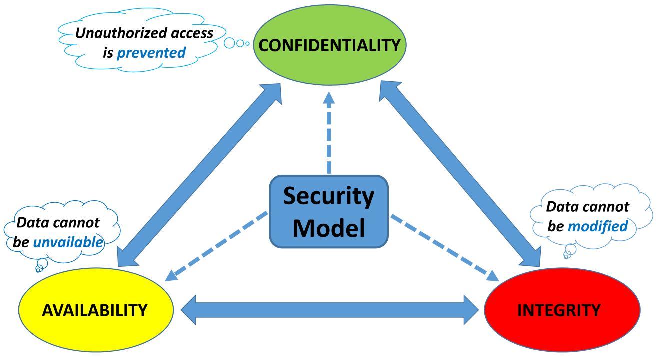

Fig. 2. CIA security model.

B. Traditional IT Security Versus IoT Security

A fundamental issue in IoT world is that most of the IoT devices are "closed," thus, customers cannot add security software once the devices have been shipped from the factory. For such reasons, security has to be built into IoT devices so that they are "secure by design" ("built-in security"). In other words, for IoT devices, the security concept must evolve from "add-on security" in which security is just added on the existing systems such as servers or PCs (traditional IT).

Another important issue is related to the fact that, in general, an IoT system is composed by nodes with limited hardware and software resources (i.e., sensor or RFID nodes), while traditional IT is mostly based on resources rich devices. So, in the IoT world, only lightweight algorithms can be used, in most of the cases, to find a right balance between higher security and lower capabilities.

In addition, the broad heterogeneity that characterizes the IoT devices is a common feature, easily observable in every functional element (identification, sensing, communication, computation, service, and semantic) [21]. In fact, in the future there will be many kinds of things potentially connecting to the Internet, ranging from cars, robots, fridges, mobile phones, to shoes, plants, watches, and so on. These kinds of things, with different technologies, will generate also large volumes of heterogeneous data poorly manageable [22]–[24]. However, the negative aspect of security is related to the increase of the attack surface: many heterogeneous technologies, coupled with their related issues, can bring also security weaknesses.

Moreover, in IoT system model, the perception layer is the most complicated to be protected because: 1) technological heterogeneity determines difficulty of using only one kind of security technology and 2) the perceptual environment is often open, and thus, security strategies, previously used in closed environments, can cause problems in the open environment. On the other side, considering the application layer, privacy issues are more challenging because IoT applications are used in our everyday life and they gather our private information every second automatically to make our life easier. In fact, these IoT applications can even control our everyday life environment and this can bring great potential security problems if

TABLE II
TRADITIONAL IT SECURITY VERSUS IOT SECURITY

Traditional IT Security	IoT Security
Add-on Security	Built-in Security
Complex algorithms	Lightweight algorithms for resource-constrained devices
User Control	Privacy issue: IoTs often collect automatically user private information
Small technological heterogeneity	Large technological heterogeneity and thus also large attack surface
Many security guards	Few security guards
IT devices are located in closed environments	IoT devices are also located in open environments

we lose control of them. Moreover, due to the lack of specific security software (e.g., antivirus and IDS), the IoT world is surely less secure than traditional IT.

In summary, IoT systems are deployed in more dangerous and heterogeneous environments with limited resources and also with less security guards. So we need to implement lightweight solutions to deal with such more dangerous environments with a large attack surface. Table II resumes the main differences between traditional IT and IoT security requirements and application contexts.

C. Multilayer and Cross Layer Security for IoT System

According to the presented IoT system model, security must be developed at different layers. Here we describe the appropriate security policies and strategies which provide a certain reference value for the practical application to IoT scenarios.

Security policies within each layer must consider the following basic mechanisms.

1) *Hardware Security:* Using cryptographic coprocessor or anti-tampering technologies (e.g., chip or memory protection, self-destruction, etc.).
2) *Access Control and Authentication System:* To prevent the access to IoT sensor nodes or application from unauthorized users.
3) *Data Encryption Mechanisms:* Guaranteed by symmetric and asymmetric encryption algorithms that should be used during data transit and storage.
4) *Secure Routing:* To ensure the correct route discovery also building and maintaining target even when network threats and attacks happen.
5) *Risk Assessment:* To discover the new system threats preventing the security breaches and determining the best security strategies.
6) *Intrusion Detection System:* To detect local and network intrusion (e.g., in WSN). It is also useful to have DDoS attack detection and prevention mechanisms.
7) *Anti-Malware Solution:* To detect and prevent malicious code update in the device firmware (e.g., sensor node) or in service or application itself.
8) *Firewall:* To block unauthorized hosts.
9) *Trust Management System:* To ensure that the security goals are enforced and the security mechanisms are successfully deployed. In this context, it is extremely useful to ensure the credibility in the relationships among IoT devices or between those devices and the users.

However, the security requirements for IoT cannot be achieved by simply putting specific solutions from each layers together. In fact, it is necessary to consider IoT system as a whole system and security can be thought of as a chain that is robust as much as its weakest link.

Therefore, to improve IoT security, we also need to have some cooperation between different layers by designing security solutions for cross layers usage overcoming heterogeneous integration issues. In this sense, interoperability [25]–[27] can become one of the enabling factors for IoT security.

V. ISSUES AND SECURITY SOLUTIONS FOR IOT COMMUNICATION PROTOCOLS

A key step to include security in IoT Systems is also related to the secure communication protocols used in a way that data in transit are confidential, reliable and available by preventing cyber attacks.

By looking the context from the protocol point of view, IoT protocols can be divided into three main levels [28]: 1) *physical access*; 2) *network*; and 3) *service and application*. In this section, we revise the most used communication protocols also describing issues and some innovative solutions proposed in the scientific literature. Table III summarizes all the considered IoT protocols and the related issues also highlighting the possible standard and novel solutions in each of the different levels.

A. Physical Access Level

This level is composed by physical and MAC layer protocols of the well known ISO/OSI architecture. In the IoT arena, the most used radio technologies to communicate are wireless such as IEEE 802.15.4, BLE, IEEE 802.11/WiFi, and LTE. While in wired networks, the communicating nodes are physically connected through cables, in wireless networks they are extremely vulnerable due to the broadcast nature of the wireless medium. Explicitly, wireless networks are prone to malicious attacks, including eavesdropping attack, DoS attack, spoofing attack, MITM attack, message falsification/injection attack, etc. Cryptographic techniques assume that the eavesdropper has limited computing power and rely upon the computational hardness of their underlying mathematical problems. Recently, physical-layer security is emerging as a promising means of protecting wireless communications to achieve information-theoretic security against eavesdropping attacks. The physical layer encryption exploits the features of the physical wireless channel for its security by communications, signal processing, and coding techniques [29].

In the following, the most common communication protocols used by IoT devices, are presented according to the radio coverage range.

1) IEEE 802.15.4: This communication standard defines the operation of low-rate wireless personal area networks. It is at the basis of the ZigBee technology. The 802.15.4 security

TABLE III
IoT PROTOCOLS: ISSUES AND SOLUTIONS

	Protocols	**Issues**	**Solutions**	**Type of Solutions**
Physical Ac. Level	*IEEE 802.15.4*	Data Transit Attacks	AES-CCM algorithms [35]	standard
	BLE	Data Transit Attacks	AES-CCM algorithms [30]	standard
		Data Transit Attacks: header information is not encrypted	Black network solution [30]	NEW
	Wi-Fi	Data Transit Attacks	WEP, WPA, WPA2 protocols [32]	standard
	LTE	Data Transit Attacks	EEA and EIA algorithms [33]	standard
Network Level	*IPv4/IPv6*	Data Transit Attacks	IPsec protocol	standard
		Threats to NDP protocol	SEND protocol in IPv6 [34]	standard
	6LoWPAN	Data Transit Attacks	Compressed IPsec protocol [35], [38]	NEW
			Compressed DTLS [35]	NEW
			802.15.4 security features [35]	standard
	RPL	Routing and DOS Attacks	SVELTE IDS solution [41]	NEW
		Data Transit Attacks	AES/CCM algorithms [40]	standard
Service & Application Level	*MQTT*	Data Transit Attacks	TLS (PSK, Certificates) [49]	standard
		Data Transit Attacks, Scalable Key management, Heavy computation cost of TLS	Secure MQTT solution with ABE [42]	NEW
		Privacy for lack of user control	SecKit solution [44], [45]	NEW
	CoAP	Data Transit Attacks	DTLS protocol (PSK, RPK, Certificates) [47]	standard
		Data Transit Attacks, Heavy cost of computation and high handshake of DTLS	Lithe solution [48]	NEW

layer is handled at the media access control layer, below the application control. The specification does not support security for acknowledgment packets; other packet types can optionally support integrity protection and confidentiality protection for packets data field. The 802.15.4 specification defines different security suites that can be classified according to the following proprieties: no security, encryption only [advanced encryption standard (AES)-CTR], authentication only (AES-CBC-MAC), and encryption and authentication (AES-CCM). The AES-CBC-MAC cipher suite ensures the authentication of the frame including a 32, 64, or 128 bits message integrity code (MIC) behind the payload. The AES-CTR enables encryption with cipher block of 128-byte length to guarantee confidentiality. The AES-CCM combines authentication with AES-CBC-MAC followed by encryption with AES-CTR.

Regarding the keys management process, three kinds of keys are defined.

1) The master key, initially predistributed to all the nodes of the network.
2) The network key shared by the legitimate nodes after authorization and authentication services provided by the upper layers.
3) The link key established between neighbor legitimate nodes.

So as requirements, the master key must be physically secured to avoid node tampering because the attacker capable to get this key can take the control of the whole IEEE 802.15.4 network [35].

2) Bluetooth Low-Energy: This communication technology uses a short range radio with a minimal amount of power to operate for a longer time (even for years) compared to its previous versions. Bluetooth low-energy (BLE) version 4.2 is more secure compared with earlier versions. In fact, it is able to create the so called LE secure connections using elliptic curve Diffie–Hellman public key cryptography which offers significantly stronger security compared to the original BLE key exchange protocol [36], [37]. In addition, BLE also provides replay protection via the SignCounter field for authenticated data over an unencrypted channel and privacy services by frequently changing the BLE device address to avoid being tracked. BLE has two primary components, the controller (PHY and link), and the host (upper layers). Message confidentiality is typically achieved by encrypting the payload portion of a frame. The header information is not encrypted. At the controller, link layer security in BLE provides confidentiality and integrity via AES-CCM. Data channel packet data units (PDUs) are authenticated with a 4-byte MIC. The encryption is done over the data channel PDU payload and the MIC. Advertising channel PDUs are not encrypted or authenticated and this provides opportunities for a range of attacks like inference attacks, eavesdropping, message modification and packet injection with incorrect control sequences. To secure all data, including the meta-data, an innovative approach is based on the *black network* concept. Adversaries should not be able to determine the source, the destination, the frame sequence number or the replay counter. The resulting link layer advertising and data PDUs are BLE compatible but with a decreased routing and payload efficiency [30]. Finally, to assess the vulnerability of BLE technology, researchers have shown that BLE technology presents high vulnerabilities due to its specific authentication mechanism [31].

3) IEEE 802.11/WiFi: The family of Wi-Fi networks mainly based on the IEEE 802.11 b/g/n standards is explosively expanding. This technology uses WEP, WPA, or WPA2 protocols to implement authentication and encryption processes. WEP uses a 64- or 128-bit encryption key that must be manually entered on wireless access points and devices and does not change while the temporal key integrity protocol (TKIP) has been adopted for WPA employing a per-packet key that dynamically generates a new 128-bit key for each packet to prevent attacks that compromised WEP. Finally, the protocol used by WPA2, based on the advanced encryption standard (AES) cipher is significantly stronger in protection for both privacy and integrity than the RC4-based TKIP used by WPA. In particular, both WPA and WPA2 use the same authentication system. Enterprise networks use EAP protocol for mutual authentication through a RADIUS server, whilst, for home and small office networks, preshared key (PSK) protocol is used. In addition, WPA adopts Michael algorithm for data integrity but WPA2 implements a more robust, efficient and stronger algorithm, CBC-MAC. In [32], a comparative study of WPA and WPA2 in terms of security methods used and throughput, is presented drawing the main conclusions on how WPA2 has less reduction on network throughput than WPA due to its encryption algorithm (CCMP) which is highly improved compared to TKIP.

4) LTE: This communication technology is the long term evolution standard for cellular technology based on the Universal Mobile Telecommunications System (UMTS). For the LTE network, two standardized algorithms are required for the radio interface, namely: 1) EPS encryption algorithm (EEA) and 2) EPS integrity algorithm (EIA). Two confidentiality and integrity algorithm sets had already been developed and standardized. The first set, 128-EEA1 and 128-EIA1, is based on the stream cipher SNOW 3G, and was inherited from the UMTS network. The second set, 128-EEA2 and 128-EIA2, is based on the block cipher AES.

3GPP Systems and Architecture Group agreed in May 2009 on a requirement for a third encryption and integrity algorithm set, 128-EEA3 and 128-EIA3, based on a core stream cipher algorithm named ZUC.

A comparative study among all core LTE cryptographic algorithms such as ZUC, SNOW 3G, and AES is provided in [33]. The results of this paper show that SNOW 3G offers less immunity against different attacks than ZUC and AES.

B. Network Level

The main functions of the network layer include message forwarding and host addressing supported by the standard ISO/OSI architecture through protocols such as IPv4/IPv6, 6LoWPAN, and routing protocol for low power and lossy networks (RPL).

1) IPv4/IPv6: IPv6 is the main enabler for extending IoT to the future Internet. In fact, IPv6 extends the existing IPv4 notation from 32 to 128 bits per IP address offering scalability for IoT world. In addition, IPv6 use mandatory end-to-end encryption, while in IPv4, it remains an extra option. IPv6 also supports more-secure name resolution achieving network layer confidentiality, integrity and authentication through IPsec protocol.

In IPv6, the secure neighbor discovery (SEND) protocol is a security extension of the neighbor discovery protocol (NDP), used in IPv6 for the discovery of neighboring nodes on the local link. NDP determines the link layer addresses of other nodes, finds available routers, maintains reachability information, performs address resolution and detects address duplication. SEND enhances this insecure protocol by employing cryptographically generated addresses (CGAs) to encrypt NDP messages. This method is independent of IPSec, which is typically used to secure IPv6 transmissions. The introduction of CGA helps to nullify neighbor/solicitation/advertisement spoofing, neighbor unreachability detection failure, DOS attacks, router solicitation, and advertisement and replay attacks. Using IPv4, it is fairly easy for an attacker to redirect traffic between two legitimate hosts and manipulate the conversation or at least observe it but IPv6 makes this very difficult [34].

2) 6LoWPAN: Since IoT system is also composed by WSNs, the Internet protocol (IP) is not suitable for such resource constrained devices. Thus, 6LoWPAN protocol provides an adaptation layer to connect the IP world to the resource constrained devices enabling the access of the sensor networks world to the Internet. In the OSI abstraction model, 6LoWPAN is an adaptation layer located between the network layer and the link layer. 6LoWPAN achieves low overhead by applying cross-layer optimization and compression of the headers of the IPv6 protocol stack.

In [35], three interesting solutions to provide security in 6LoWPAN networks are proposed and discussed.

1) Using security features of IEEE 802.15.4 (link layer security).
2) Compressed IPsec to provide end-to-end security at the network layer also using header compression techniques [38].
3) Compressed DTLS to provide end-to-end security at the transport layer. A specific technique to compress DTLS header in a standard compliant way into a 6LoWPAN network can be used to achieve better energy efficiency by reducing the message size.

The main difference among these solutions is that link layer security ensures the security of the wireless medium, whereas upper layer security is designed to achieve end-to-end security between two peers.

3) RPL: It is a standardized routing protocol for the IP-connected IoT devices. It creates a destination-oriented directed acyclic graph (DODAG) and supports different modes of operation: unidirectional traffic to a DODAG root (typically the 6BR/border router) and bi-directional traffic between constrained nodes and a DODAG root. Nodes have a rank that determines their individual position with respect to the DODAG root and relative to other nodes.

The RPL specification [39] defines secure versions of the various routing control messages, as well as three basic security modes. In the first mode, named "unsecured," RPL control messages are sent without any additional security mechanisms. In the second mode, called "preinstalled," nodes joining an

RPL instance have preconfigured symmetric key that enable them to process and generate secured RPL messages. The third mode, named "authenticated," it is used for devices operating as routers. A device may initially join the network using a preconfigured key and the preinstalled security mode, and next obtain a different cryptographic key from a key authority with which it may start functioning as a router. The key authority is responsible for authenticating and authorizing the device for this purpose. Each RPL message has a secure variant and AES/CCM algorithms [40] are used to support confidentiality and integrity.

Even with message security that enables encryption and authentication, networks are vulnerable to a number of wireless and routing attacks aimed to disrupt the network. Hence, an IDS is necessary to detect intruders that are trying to disrupt the network. In [41], a novel IDS for IoT systems is presented. This IDS called SVELTE is well designed for 6LowPAN networks with RPL in which a hybrid, centralized and distributed approach is used to place IDS modules both in the 6BR and in the resource constrained nodes. SVELTE has three main centralized modules developed in the 6BR. The first module, called 6LoWPAN mapper, gathers information about the RPL network and reconstructs the network in the 6BR. The second module is the intrusion detection component that analyzes the mapped data and detects intrusion. The third module, a distributed mini-firewall, is designed to offload nodes by filtering unwanted traffic toward resource-constrained network.

C. Service and Application Level

As a result of the wide-spread and rapid evolution of IoT devices, different protocols have been developed in order to support the emerging M2M data communications such as MQTT, constrained application protocol (CoAP), XMPP, and AMQP.

In this section, we discuss issues and some innovative solutions proposed by researchers for the two most widely used application protocols: 1) MQTT and 2) CoAP. In particular, these protocols overcomes other solutions in terms of minimum header size, power consumption, and data loss; thus, they are well suited for constrained-resource applications [21].

1) Message Queuing Telemetry Transport: This protocol is a publisher/subscriber messaging protocol specifically developed for constrained devices. Message queuing telemetry transport (MQTT) security is based on the TLS/SSL to provide transport encryption. It provides a security against eavesdropping. On the application layer, MQTT application provides client identifier and username/password credentials which can be used for devices authentication. The disadvantage of MQTT security is the use of TLS/SSL which is not optimized for constrained devices. In fact, using TLS/SSL with certificates and session key management for a multitude of heterogeneous devices, is surely cumbersome [42]. For this reasons, a more scalable, lightweight, and robust security mechanism is required.

In [42] a secure MQTT (SMQTT) is proposed to increase security features of the existing MQTT protocol and its variants based on lightweight attribute-based encryption (ABE), over elliptic curves. The advantage of using ABE is due to its inherent design which supports broadcast encryption (one encryption message delivered to multiple intended users) that make it suitable for IoT applications; moreover, the feasibility of SMQTT approach through simulations and performance evaluation has been validated.

In [43], two different types of ABEs, key-policy ABE and ciphertext-policy ABE, have been evaluated on different classes of mobile devices including a laptop and a smartphone providing a comprehensive study of ABE techniques and their performances. Compared to the RSA (an asymmetric cryptographic algorithm), ABE is slower and has more data overhead and energy consumption; however, the main advantage to use ABE is to enable a flexible and fine grained access control and to offer scalable key management because senders and receivers are completely decoupled.

In IoT world, protection of privacy can be a challenging task because connected objects can generate an enormous amount of data, some of which actually constitute personal data. In addition, it is difficult to control the data flow without having any user interface or adequate tools for the user. An efficient solution to enforce security policy rules in IoT is described in [44] and [45]. This enforcement solution consists of a model-based security toolkit named SecKit that is integrated within the MQTT protocol. The policy enforcement support for MQTT is based on a custom policy enforcement point (PEP) component implemented in *C* language. The PEP is a connector that: 1) intercepts the messages exchanged inside the broker with a publish-subscribe mechanism; 2) notifies these messages as events in the SecKit policy decision point implemented in Java; and optionally 3) receives an enforcement action (allow, deny, modify, and delay) to be executed. In addition, this PEP has been embedded in the *Mosquitto Broker* [46] using security plugin. The following list summarizes advantages of this solution respect to the missing features in current MQTT implementations.

1) Modification of messages and identity obfuscation.
2) Delaying of messages to prevent real-time tracking of devices and users.
3) Enforcement when a message is delivered to a client in addition to enforcement when a client subscribes a topic.
4) Support for reactive rules to notify, log, or request user consent.
5) Misbehavior checking rules, for DoS attack detection.

The main drawback of this approach is the high overhead when one publisher has many interested subscribers, and a policy needs to be checked for every subscriber. This overhead introduces a small latency of a few tens of ms.

2) Constrained Application Protocol: The protocol is an HTTP remarkable version to match the IoT requirements for low overhead. The CoAP uses UDP protocol and encryption is most commonly accomplished using DTLS and sometimes with IPSec. DTLS is applied in the transport layer and the fundamental AES/CCM provides confidentiality, integrity, authentication, and nonrepudiation.

The *Californium* framework (implemented in Java) provides a set of security capabilities for CoAP. There are four security modes defined for CoAP to implement TLS [47].

1) *No security*.

2) *PSK* enabled by sensing devices preprogrammed with symmetric cryptographic keys. This mode is suitable for devices that are unable to support the public key cryptography.
3) *Raw public key (RPK)* for devices that require authentication based on public key. This mode enables a TLS session without certificate.
4) *Certificates* to support authentication based on public key where keys are always validated according to a trusted entity known as certificate authority. The drawback of using the certificates is mainly due to heavy data format and fixed costs. A clear advantage, however, is the possibility to revoke certificates if the device is compromised.

Key management is a drawback of the CoAP security which is a common issue in almost all protocols. Another problem is the heavy cost of computation and high handshake in the message which causes message fragmentation. Many studies proposed different solutions to compress the DTLS. In fact, a novel DTLS header compression scheme called *Lithe* has been proposed in [48] with the aim of significantly reducing the energy consumption by leveraging the 6LoWPAN standard without compromising the end-to-end security properties. In addition, the evaluation results show significant gains in terms of packet size, energy consumption, processing time, and network-wide response times when compressed DTLS is enabled. A clear limitation of this solution is that DTLS header compression is applied only within 6LoWPAN networks.

In [49], a security analysis between CoAP and MQTT is presented with a particular focus on the transport level protocol used (UDP for CoAP and TCP for MQTT), which inherently enforces the usage of DTLS for CoAP and TLS for MQTT. Moreover a set of security modes and also mandatory-to-implement ciphers are supported by CoAP whilst, in contrast, the MQTT specification only enumerates a list of security considerations and does not enforce any kind of implementations. The comparative analysis has been conducted considering the four security modes already described. According to this analysis, RPK is not supported by MQTT, but it represents a mixed security alternative to heavier certificates and lightweight PSKs. However, the traditional certificates-based authentication and encryption offers the highest level of security. Furthermore, the possibility to revoke certificates, considering illicit usage, makes it more capable to react to different attacks as already been proven with HTTP. In addition, due to different standard security mechanisms, the interoperability issue has a non trivial solution, mostly based on security level negotiation between IoT devices.

VI. Critical Issues and Future Directions

To direct further research on the most vulnerable layer of IoT system model, we can use risk classification limited to a qualitative evaluation of each layer due to lack of quantitative metrics.

The *perception layer* can be classified with the highest security risk level for physical exposure of IoT devices, deployed also in open environments. In addition, it has very large hardware limitations and technological heterogeneity that limit the implementation of effective security measures.

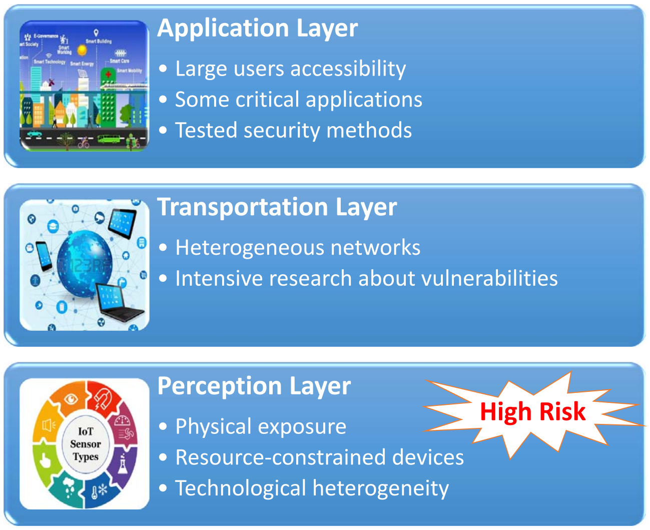
Application Layer
• Large users accessibility
• Some critical applications
• Tested security methods
Transportation Layer
• Heterogeneous networks
• Intensive research about vulnerabilities
Perception Layer
• Physical exposure
• Resource-constrained devices
• Technological heterogeneity
High Risk
IoT Sensor Types

Fig. 3. Qualitative risk evaluation for IoT system.

On the other side, the *transportation layer* can be classified as a lower risk level respect to the perception layer due to the known drawbacks of standard wireless data transfer technologies, as well as known threats in access networks. The advantage of this layer is the intensive research on the vulnerabilities and the continuous development of new protection methods.

Finally, the *application layer* has a "variable" level of risk depending on the specific implemented application; in fact, this layer is generally accessible from a large number of users and in some IoT applications, the impact of both data and services confidentiality, integrity, or availability losses, can be significant and not tolerable (i.e., strategic sectors such as energy sector or intelligent transportation systems). In addition, compared to the perception layer, it has more mature technology, less threats, and already tested security methods.

Fig. 3 graphically resumes this qualitative risk evaluation for each layer of the IoT system.

A. Critical Security Issues Identification

According to the previous analysis, the most vulnerable layer of the presented IoT system model is the perception layer and the critical issues to solve in next future are as follows.

1) *Hardware InSecurity of IoT Devices:* This issue depends on device manufacturers's negligence.
2) *Lack of Lightweight Cryptographic Algorithms and Effective Key Management:* Protecting data confidentiality and integrity at rest or in transit.
3) *Lack of Lightweight Trust Management System:* It is important to ensure credibility especially in the relationships between IoT devices placed in open and dynamic environments.
4) *InSecure Routing Protocols:* Providing protection against routing threats with specific focus on the WSNs.
5) *Lack of Lightweight Anti-Malware Solutions:* Providing protection from malware that can infect the software installed on the IoT device.

TABLE IV
METRIC VALUES AND BS FOR CRITICAL AND OPEN ISSUES IN IOT SYSTEM

Issue	Values of Metric	Justification	BS
Hardware InSecurity	AV:Local	The attacker must either have physical access to the vulnerable device	7.2
	AC: Low	IoT devices are deployed in open environments and thus easily accessible	
	Au:None	There is no requirement for the attacker to authenticate.	
	C, I, A: Complete	The impact for IoT System can be complete	
Lack of Lightweight Cryptographic algorithms	AV:Adjacent Network	The attacker can gain access to this vulnerability through a not-encrypted local network	8.0
	AC: Low	IoT devices are deployed in open environments and thus easily accessible	
	Au:None	There is no requirement for the attacker to authenticate.	
	C, I:Complete	The information confidentiality and integrity are not guaranteed	
	A:Partial	The impact of Availability for IoT System is less than the first two parameters	
Lack of Lightweight Trust Management System	AV:Adjacent Network	The attacker can make impersonation attacks in the percepual networks (e.g. WSN)	8.3
	AC: Low	There are no special requirements for access	
	Au:None	There is no requirement for the attacker to authenticate.	
	C, I, A:Complete	The attacker can completely read, alter or make unavailable informations	
Lack of Lightweight Secure Routing Protocols	AV:Adjacent Network	The attacker can be use a local network to make routing attacks	5.8
	AC: Low	There are no special requirements for access	
	Au:None	There is no requirement for the attacker to authenticate.	
	C, I, A:Partial	The attacker can read, alter or make unvailable some informations	
Lack of Lightweight Anti-malware Solutions	AV: Network	A remote attacker can inject malware in IoT device	9.3
	AC: Medium	There are some special requirements for access (e.g. exploit some sw vulnerabilities)	
	Au:None	There is no requirement for the attacker to authenticate.	
	C, I, A:Complete	The attacker can completely read, alter or make unavailable informations	
Physical Wireless InSecurity	AV:Adjacent Network	The attacker can gain access broadcast wireless channel	5.8
	AC: Low	Wireless channel is easily accessible in proximity of an adjacent network	
	Au:None	There is no requirement for the attacker to authenticate.	
	C, I, A:Partial	These parameters are partially guaranteed	
DDoS Attack Issue	AV:Adjacent Network	The attacker must be in the adjacent network	6.1
	AC: Low	Wireless channel is easily accessible in proximity of an adjacent network	
	Au:None	There is no requirement for the attacker to authenticate.	
	C, I:None	These parameters are not interested	
	A:Complete	DDoS attack hacks availability of network services	
Common App Vulnerabilities	AV: Network	A remote attacker can exploit these vulnerabilities	9.3
	AC: Medium	There are some special requirements exploit some sw vulnerability	
	Au:None	In the worst case, there is no requirement for the attacker to authenticate.	
	C, I, A:Complete	The attacker can completely read, alter or make unavailable informations	
Privacy Protection Issue	AV: Network	The attacker can remotely access to user data	7.8
	AC: Low	In IoT applications, there are usually not used privacy protection mechanisms	
	Au:None	There is no requirement for the attacker to authenticate.	
	C:Complete	The information confidentiality is not guaranteed	
	I, A:None	These parameters are not interested	

Regarding the transportation layer, since it is composed by a mixed wireless network technologies, the most critical and open issues to be addressed are as follows.

1) *Physical Wireless InSecurity:* The broadcast nature of wireless communications makes the physical channel extremely vulnerable to classic data transit attacks [29].
2) *DDoS Attacks:* Because of the heterogeneity and complexity of the IoT networks, the transportation layer is vulnerable and exposed to this kind of attacks. Usually the solution is to upgrade the system and use DDoS attack detection and prevention. Currently, there is no good solution to solve the network DDoS attack.

Finally, the application layer represents the most variegate security context, in fact, different security requirements need to be satisfied for different applications; for instance, the security of data privacy would be of great importance in smart healthcare, but in intelligent urban management, data authenticity and integrity would be more important. Moreover, at the present time, there are no universal standards for the developing of IoT application layer making very difficult the interoperability among them (e.g., different software and applications have different authentication mechanisms, which makes integration of all of them very difficult to ensure data privacy and identity authentication).

At this layer the most serious issues that must be considered are as follows.

1) *Common Application Vulnerabilities:* These vulnerabilities can be exploited by an attacker to hack an application service. In this context, the Open Web Application Security Project [53], [55] provides a list of critical

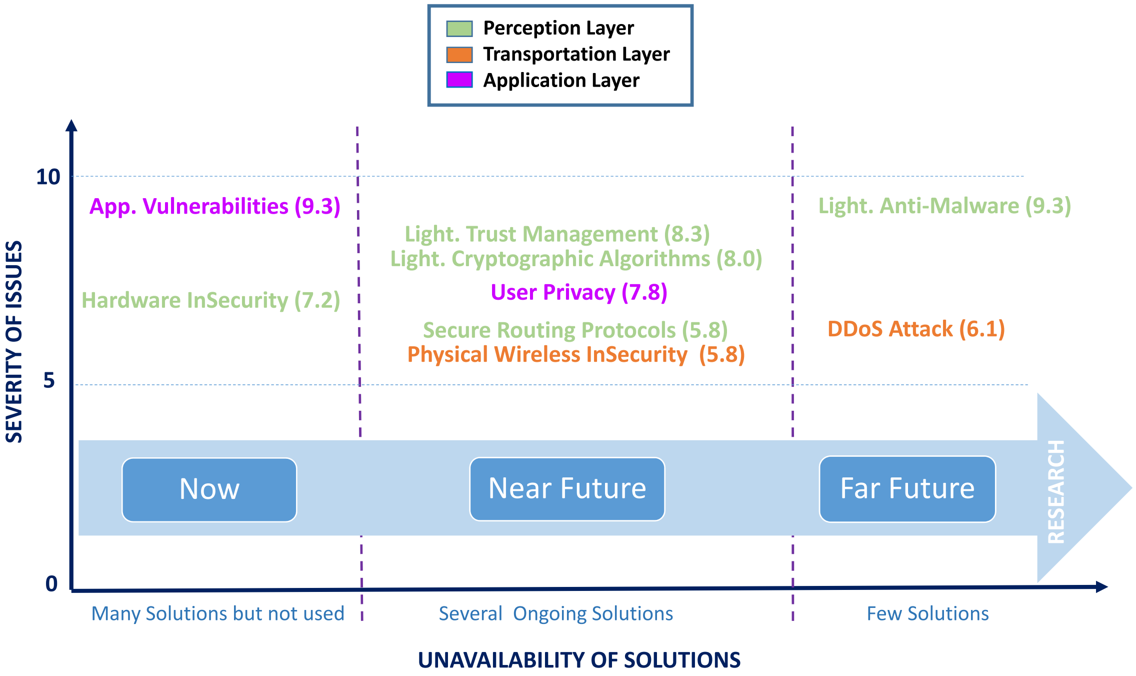

Fig. 4. Research direction.

and common software vulnerabilities for Web application or cloud services, coupled with few possible solutions.

2) *Privacy Protection Issue:* It is necessary to provide user data protection mechanisms in which user can also transparently enforce own privacy preferences [54].

B. Critical Security Issues Evaluation

To evaluate the presented critical security issues, with the aim of directing the research activities in the next future, we considered them as intrinsic vulnerabilities of the IoT Systems and we calculated a severity score for each of them by using a novel approach through conventional base score (BS) equations named common vulnerability scoring system (CVSS) v2, proposed by the National Infrastructure Advisory Council [50], [51]. CVSS is a free and open industry standard for assessing the severity of computer system security vulnerabilities. It attempts to assign severity scores to different vulnerabilities, allowing managers to prioritize responses and resources according to the specific threat. Scores are calculated according to several metrics that approximate ease of exploit and the impact of exploit. Scores range from 0 to 10, with 10 being the most severe.

The BS shown in (1) is composed of two sets of metrics: 1) the *exploitability* metrics and 2) the *impact* metrics.

The *exploitability metrics* capture how the vulnerability is accessed and whether or not extra conditions are required to exploit it. These metrics are as follows.

1) The access vector (AV) that shows how a vulnerability may be exploited.
2) The access complexity (AC) metric that describes how easy or difficult it is to exploit the discovered vulnerability.
3) The authentication (Au) metric that describes the number of times that an attacker must authenticate to a target to exploit it.

$$\begin{aligned}\text{BS} = {} & (0.6 * \text{Impact} + 0.4 * \text{Exploitability} - 1.5)\\ & * f(\text{Impact}). \qquad (1)\end{aligned}$$

The *impact metrics* measure how a vulnerability, if exploited, will directly affect an IT asset, where the impacts are independently defined as the degree of loss of confidentiality (C), integrity (I), and availability (A).

To calculate these sets of metrics, the following mathematical equations have been used:

$$\text{Exploitability} = 20 * \text{AC} * \text{Au} * \text{AV}$$
$$\text{Impact} = 10.41 * (1 - (1 - C) * (1 - I) * (1 - A))$$

where

$$f\ (\text{Impact}) = 0 \text{ if Impact} = 0$$
$$f\ (\text{Impact}) = 1.176 \text{ otherwise.}$$

The possible values of the six base metrics are shown in Table V and they are chosen considering the characteristics of each specific security issue.

Table IV resumes the results obtained by applying the CVSSv2 metrics to the security open issues identified in the proposed IoT system. In particular, to compute the BS, we have used CVSSv2 calculator, freely provided by National Institute of Standards and Technology [52].

Once computed the BS, the security issues have been sorted according to the availability of the solutions to better understand in which direction the research must be oriented. By looking Fig. 4 that graphically resume the conducted analysis, the following meaningful considerations can be done.

1) *Hardware insecurity* and *common application vulnerabilities* have already many mature solutions. However, the real applicability of those solutions

TABLE V
BASE METRICS WITH SUBSCORES

Base Metrics	Sub-score
AV	Local=0.395
	Adjacent Network=0.646
	Network=1.000
AC	High=0.350
	Medium=0.610
	Low=0.710
Au	Multiple=0.450
	Single=0.560
	None=0.704
C *or* I *or* A	None=0.000
	Partial=0.275
	Complete=0.660

strictly depends on device manufacturers or software developers that should be forced to implement them.

2) *Lack of lightweight anti-malware* and *DDoS attack issue* have few research solutions although they can have a medium-high severity index.
3) The remaining security issues have several on going solutions but still immature.

According to these considerations, the research activity in the near future, should concentrate to solve critical issues with greater availability of ongoing solutions that are progressively more feasible thanks to the technology advancements.

VII. CONCLUSION

Along with the rapid development of the IoT industry, the importance of the security in the IoT is gradually emerging. In fact, we have shown that IoT system model has many security issues among which threats that can exploit some possible weaknesses. For these reasons, it is necessary to appropriately enforce *trust management* and *security* in the IoT world starting from the characterization of the different threats related to each specific level of the general IoT system model.

According to this paper, the most vulnerable level of the IoT system model is the perception layer due to the physical exposure of IoT devices, to their constrained resources and to their technological heterogeneity. Thus, it is crucial, in the next future, to start working on the critical issues of this level implementing lightweight security solutions that can adapt to the heterogeneous environments with resource-constrained devices.

REFERENCES

[1] S. Karnouskos, P. J. Marrón, G. Fortino, L. Mottola, and J. R. Martínez-de Dios, *Applications and Markets for Cooperating Objects* (Springer Briefs in Electrical and Computer Engineering). Heidelberg, Germany: Springer, 2014, pp. 1–120.

[2] G. Fortino and P. Trunfio, *Internet of Things Based on Smart Objects, Technology, Middleware and Applications*. Cham, Switzerland: Springer, 2014.

[3] H. Xiao, N. Sidhu, and B. Christianson, "Guarantor and reputation based trust model for social Internet of Things," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Dubrovnik, Croatia, 2015, pp. 600–605.

[4] *Inter-IoT Project*. Accessed: Oct. 2017. [Online]. Available: http://www.inter-iot-project.eu/

[5] Wikipedia Contributors. (2016). *Dyn Cyberattack*. [Online]. Available: https://en.wikipedia.org/w/index.php?title=2016_Dyn_cyberattack&oldid=763071700

[6] E. Ronen, A. Shamir, A.-O. Weingarten, and C. O'Flynn, "IoT goes nuclear: Creating a ZigBee chain reaction," in *Proc. IEEE Symp. Security Privacy (SP)*, San Jose, CA, USA, 2017, pp. 195–212.

[7] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, Nov. 2014.

[8] K. Lin, M. Chen, J. Deng, M. M. Hassan, and G. Fortino, "Enhanced fingerprinting and trajectory prediction for IoT localization in smart buildings," *IEEE Trans. Autom. Sci. Eng.*, vol. 13, no. 3, pp. 1294–1307, Jul. 2016.

[9] S. Baraković *et al.*, "Security issues in wireless networks: An overview," in *Proc. XI Int. Symp. Telecommun. (BIHTEL)*, Sarajevo, Bosnia and Herzegovina, 2016, pp. 1–6.

[10] P. De Meo, K. Musial-Gabrys, D. Rosaci, G. M. L. Sarnè, and L. Aroyo, "Using centrality measures to predict helpfulness-based reputation in trust networks," *ACM Trans. Internet Technol.*, vol. 17, no. 1, pp. 1–20, 2017.

[11] W.-Y. Lin, X. Zhang, H. Song, and K. Omori, "Health information seeking in the Web 2.0 age: Trust in social media, uncertainty reduction, and self-disclosure," *Comput. Human Behav.*, vol. 56, pp. 289–294, Mar. 2016.

[12] H. Shirgahi, M. Mohsenzadeh, and H. H. S. Javadi, "Trust estimation of the semantic Web using semantic Web clustering," *J. Exp. Theor. Artif. Intell.*, vol. 29, no. 3, pp. 537–556, 2017.

[13] T. S. Vijay, S. Prashar, and C. Parsad, "Online shoppers' satisfaction: The impact of shopping values, website factors and trust," *Int. J. Strategic Decis. Sci.*, vol. 8, no. 2, pp. 52–69, 2017.

[14] S. Pinto, T. Gomes, J. Pereira, J. Cabral, and A. Tavares, "IIoTEED: An enhanced, trusted execution environment for industrial IoT edge devices," *IEEE Internet Comput.*, vol. 21, no. 1, pp. 40–47, Jan./Feb. 2017.

[15] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "ReTrust: Attack-resistant and lightweight trust management for medical sensor networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 4, pp. 623–632, Jul. 2012.

[16] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, Jun. 2014.

[17] G. Lize, W. Jingpei, and S. Bin, "Trust management mechanism for Internet of Things," *China Commun.*, vol. 11, no. 2, pp. 148–156, Feb. 2014.

[18] I.-R. Chen, F. Bao, and J. Guo, "Trust-based service management for social Internet of Things systems," *IEEE Trans. Depend. Secure Comput.*, vol. 13, no. 6, pp. 684–696, Nov./Dec. 2016.

[19] I. Kounelis *et al.*, "Building trust in the human–Internet of Things relationship," *IEEE Technol. Soc. Mag.*, vol. 33, no. 4, pp. 73–80, Nov. 2014.

[20] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and security in Internet of Things and wearable devices," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 1, no. 2, pp. 99–109, Apr./Jun. 2015.

[21] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[22] X. Xu, R. Ansari, A. Khokhar, and A. V. Vasilakos, "Hierarchical data aggregation using compressive sensing (HDACS) in WSNs," *ACM Trans. Sensor Netw.*, vol. 11, no. 3, 2015, Art. no. 45.

[23] Y. Qin *et al.*, "When things matter: A survey on data-centric Internet of Things," *J. Netw. Comput. Appl.*, vol. 64, pp. 137–153, Apr. 2016.

[24] J. Wan *et al.*, "Software-defined industrial Internet of Things in the context of industry 4.0," *IEEE Sensors J.*, vol. 16, no. 20, pp. 7373–7380, Oct. 2016.

[25] G. Aloi *et al.*, "Enabling IoT interoperability through opportunistic smartphone-based mobile gateways," *J. Netw. Comput. Appl.*, vol. 81, pp. 74–84, Mar. 2017.

[26] R. Gravina, C. E. Palau, M. Manso, A. Liotta, and G. Fortino, *Integration, Interconnection, and Interoperability of IoT Systems*. Cham, Switzerland: Springer, 2018.

[27] G. Aloi *et al.*, "A mobile multi-technology gateway to enable IoT interoperability," in *Proc. IEEE 1st Int. Conf. Internet Things Design Implement. (IoTDI)*, Berlin, Germany, 2016, pp. 259–264.

[28] Z. Sheng *et al.*, "A survey on the IETF protocol suite for the Internet of Things: Standards, challenges, and opportunities," *IEEE Wireless Commun.*, vol. 20, no. 6, pp. 91–98, Dec. 2013.

[29] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[30] S. Chakrabarty and D. W. Engels, "Black networks for Bluetooth low energy," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Las Vegas, NV, USA, 2016, pp. 11–14.

[31] Y. Qu and P. Chan, "Assessing vulnerabilities in Bluetooth low energy (BLE) wireless network based IoT systems," in *Proc. IEEE 2nd Int. Conf. Big Data Security Cloud (BigDataSecurity)*, New York, NY, USA, 2016, pp. 42–48.

[32] A. H. Adnan *et al.*, "A comparative study of WLAN security protocols: WPA, WPA2," in *Proc. Int. Conf. Adv. Elect. Eng. (ICAEE)*, Dhaka, Bangladesh, 2015, pp. 165–169.

[33] A. G. Sulaiman and I. F. Al Shaikhli, "Comparative study On 4G/LTE cryptographic algorithms based on different factors," *Int. J. Comput. Sci. Telecommun.*, vol. 5, no. 7, pp. 7–10, Jul. 2014.

[34] Y. E. Gelogo, R. D. Caytiles, and B. Park, "Threats and security analysis for enhanced secure neighbor discovery protocol (SEND) of IPv6 NDP security," *Int. J. Control Autom.*, vol. 4, no. 4, pp. 179–184, 2011.

[35] C. Hennebert and J. D. Santos, "Security protocols and privacy issues into 6LoWPAN stack: A synthesis," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 384–398, Oct. 2014.

[36] (Dec. 2014). *Bluetooth Core Version 4.2*. [Online]. Available: https://www.bluetooth.com/specifications/adopted-specifications

[37] *A Basic Introduction to BLE Security*. Accessed: Nov. 2016. [Online]. Available: https://eewiki.net/display/Wireless/A+Basic+Introduction+to+BLE+Security

[38] S. Raza *et al.*, "Securing communication in 6LoWPAN with compressed IPsec," in *Proc. Int. Conf. Distrib. Comput. Sensor Syst. Workshops (DCOSS)*, Barcelona, Spain, 2011, pp. 1–8.

[39] "RPL: IPv6 routing protocol for low-power and lossy networks," Internet Eng. Task Force, Fremont, CA, USA, RFC 6550, 2012. [Online]. Available: https://tools.ietf.org/html/rfc6550

[40] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.

[41] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2661–2674, Nov. 2013.

[42] M. Singh, M. A. Rajan, V. L. Shivraj, and P. Balamuralidhar, "Secure MQTT for Internet of Things (IoT)," in *Proc. 5th Int. Conf. Commun. Syst. Netw. Technol.*, Gwalior, India, 2015, pp. 746–751.

[43] X. Wang, J. Zhang, E. M. Schooler, and M. Ion, "Performance evaluation of attribute-based encryption: Toward data privacy in the IoT," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Sydney, NSW, Australia, 2014, pp. 725–730.

[44] R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the Internet of Things," in *Proc. IEEE 10th Int. Conf. Wireless Mobile Comput. Netw. Commun. (WiMob)*, Larnaca, Cyprus, 2014, pp. 165–172.

[45] R. Neisse, G. Steri, I. N. Fovino, and G. Baldini, "SecKit: A model-based security toolkit for the Internet of Things," *Comput. Security*, vol. 54, pp. 60–76, Oct. 2015.

[46] *Mosquitto: An Open Source MQTT v3.1/v3.1.1 Broker*. Accessed: Oct. 2017. [Online]. Available: https://mosquitto.org/

[47] R. A. Rahman and B. Shah, "Security analysis of IoT protocols: A focus in CoAP," in *Proc. 3rd MEC Int. Conf. Big Data Smart City (ICBDSC)*, Muscat, Oman, 2016, pp. 1–7.

[48] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight secure CoAP for the Internet of Things," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3711–3720, Oct. 2013.

[49] S. Zamfir, T. Balan, I. Iliescu, and F. Sandu, "A security analysis on standard IoT protocols," in *Proc. Int. Conf. Appl. Theor. Electricity (ICATE)*, Craiova, Romania, 2016, pp. 1–6.

[50] *CVSS*. Accessed: Mar. 2017. [Online]. Available: https://en.wikipedia.org/wiki/CVSS

[51] *CVSSv2*. Accessed: Mar. 2017. [Online]. Available: https://www.first.org/cvss/v2/guide

[52] *Common Vulnerability Scoring System Version 2 Calculator*. Accessed: Mar. 2017. [Online]. Available: https://nvd.nist.gov/CVSS/CVSS-v2-Calculator

[53] *OWASP Project*. Accessed: Mar. 2017. [Online]. Available: https://www.owasp.org/ index.php/OWASP_Internet_of_Things_Project

[54] *The Internet of Things (IoT): An Overview*. Accessed: Mar. 2017. [Online]. Available: https://www.internetsociety.org/doc/iot-overview

[55] J. Ahamed and A. V. Rajan, "Internet of Things (IoT): Application systems and security vulnerabilities," in *Proc. 5th Int. Conf. Electron. Devices Syst. Appl. (ICEDSA)*, Ras al-Khaimah, UAE, 2016, pp. 1–5.

Mario Frustaci received the master's degree in electronic engineering in 2014 and the postgraduate degree in cyber security. He is currently pursuing the Ph.D. degree in telecommunications engineering at the Department of Informatics, Modeling, Electronics and System Engineering, University of Calabria, Rende, Italy.

His current research interests include security, privacy, and interoperability for Internet of Things.

Pasquale Pace (M'05) received the Ph.D. degree in information engineering from the University of Calabria (Unical), Rende, Italy, in 2005.

He was a Visiting Researcher with CCSR, Surrey, U.K., and the Georgia Institute of Technology, Atlanta, GA, USA. He is currently an Assistant Professor of telecommunications with Unical. He has authored over 80 papers in international publications. His current research interests include cooperative communications, cognitive networks, sensor and self-organized networks, and interoperability of Internet of Things platforms and devices.

Gianluca Aloi (S'99–M'02) received the Ph.D. degree in systems engineering and computer science with the DEIS Department, University of Calabria (Unical), Rende, Italy, in 2003.

In 2004, he joined Unical, where he is currently an Assistant Professor of telecommunications with the Department of Informatics, Modeling, Electronics and System Engineering. His current research interests include spontaneous and reconfigurable wireless networks, cognitive and opportunistic networks, sensor and self-organizing wireless networks, and Internet of Things technologies.

Giancarlo Fortino (SM'12) received the Ph.D. degree in computer engineering from the University of Calabria (Unical), Rende, Italy, in 2000.

He is a Professor of computer engineering with the Department of Informatics, Modeling, Electronics, and Systems, Unical. He is the co-founder and the CEO of SenSysCal S.r.l., Rende, a Unical spin-off focused on innovative Internet of Things (IoT) systems. He has authored over 300 papers in international journals, conferences, and books. His current research interests include agent-based computing, wireless sensor networks, and IoT technology.