



## Internet of things: Survey on security

Diego Mendez Mena, Ioannis Papapanagiotou & Baijian Yang

To cite this article: Diego Mendez Mena, Ioannis Papapanagiotou & Baijian Yang (2018): Internet of things: Survey on security, Information Security Journal: A Global Perspective, DOI: [10.1080/19393555.2018.1458258](https://doi.org/10.1080/19393555.2018.1458258)

To link to this article: <https://doi.org/10.1080/19393555.2018.1458258>



Published online: 04 Apr 2018.



Submit your article to this journal [↗](#)



View related articles [↗](#)



View Crossmark data [↗](#)



## Internet of things: Survey on security

Diego Mendez Mena <sup>a</sup>, Ioannis Papapanagiotou <sup>b,c</sup>, and Baijian Yang <sup>c</sup>

<sup>a</sup>Center for Education and Research in Information Security and Assurance, Purdue University, West Lafayette, IN, USA; <sup>b</sup>Netflix Inc., Los Gatos, CA, USA; <sup>c</sup>Department of Computer and Information Technology, Purdue University, West Lafayette, IN, USA

### ABSTRACT

The Internet of things (IoT) is intended for ubiquitous connectivity among different entities or “things”. While it provides effective and efficient solutions to many real world challenges, the security aspect of it has always been questioned. The situation is further exacerbated by the number of connected devices growing exponentially. As a result, security and privacy has emerged as a significant challenge for the IoT. In this paper, we aim to provide a thorough survey on IoT security and privacy challenges from the perspective of technologies and architecture used. This work focuses on IoT intrinsic vulnerabilities and their implications to the fundamental information security challenges in confidentiality, integrity, and availability. The approach of this survey is to summarize and synthesize published work in IoT; relate it to the security conjuncture of the field; and project future research directions.

### KEYWORDS

Availability; confidentiality; integrity; Internet of things; security



## Introduction

The essence of the Internet of Things (IoT) resides on the concept of a wide variety of devices that connect and share data at any level in synergy with the current Internet framework. The IoT defines embedded devices capable of interacting with users and other devices over a network infrastructure with limited or nonexistent user interaction. There is a seamless integration between us and the “things” around us. This means that devices become part of our experience. Every device is connected to every other device, communicating with one another, transferring and retrieving data, intelligently responding, and triggering actions.

The successful implementation of the IoT requires the consideration of a number of important factors including but not limited to the communication technologies, communication protocols, hardware and embedded devices, and the software. A significant surge of IoT devices has been recorded in the past few years and the tendency seems to continue. It is predicted that by the end of 2020 there will be around 20 billion connected devices (Gartner, 2015). The data exchanged over the network will be greater than 40 Zettabytes for the same period (Forbes, 2016). This

brings up an important discussion regarding the security of the data generated, stored, and transmitted by IoT devices and the privacy of the users who produced or consumed the data. Every approach of IoT system must be secure and provide the necessary controls and privacy to the users. Successful implementation of an IoT system is possible only when the security and privacy are built, rather than adding the protection as a “decoration” layer on top of an IoT system.

This paper discusses the security issues at different levels of IoT systems. Section II describes the IoT architecture and current standardization efforts. Section III provides a high-level overview of current security problems and environment. Section IV presents a dive-in view of the current IoT enabling technologies and protocols focused on each of the layers of the IoT architecture. Section V discusses the IoT security concerns under the security triad perspective and explores some of the current privacy issues of the IoT from a few different points of view. Finally, Section VI summarizes the ongoing security challenges in IoT and lays out a few promising approaches.

**CONTACT** Diego Mendez Mena  [dmendezm@purdue.edu](mailto:dmendezm@purdue.edu)  Center for Education and Research in Information Security and Assurance, Purdue University, West Lafayette, IN, USA.

Color versions of one or more of the figures in the article can be found online at [www.tandfonline.com/uiss](http://www.tandfonline.com/uiss).

## Structure of IoT systems

The IoT is heterogeneous in nature. The dynamics, intelligence, and mobility of IoT makes it a high-demand technology but also makes the IoT vulnerable and risky under security terms. The different platforms where the IoT is available make it even more difficult for security researchers to find comprehensive solutions to the current security challenges. Therefore, the importance of understanding the foundation and the components of the IoT becomes paramount.

The foundation of ubiquitous computing, which is fundamental to the IoT, is made up of three components (Gubbi, Buyya, Marusic, & Palaniswami, 2013): (a) Hardware, (b) Middleware, and (c) Presentation. According to Atzori, Iera, and Morabito (2010) and Gubbi et al. (2013), three factors are attributed to the IoT environment, as illustrated in Figure 1. The IoT architecture, according to K. Zhao and Ge (2013) is composed of three layers: Perception, Network, and Application, also pictured in Figure 1. The perception layer gathers environmental data. The network layer, which is composed of wired and wireless systems, processes, and transmits the input obtained by the perception layer supported by technological platforms. The application layer consists of abstracted solutions that interact

with the final users in order to satisfy their needs. The IoT requires architectural solutions that can manage heterogeneous states in order to work efficiently and effectively (Weyrich & Ebert, 2016).

However, there is no unified view of the IoT framework. Some engineering bodies, including the Institute of Electrical and Electronics Engineers (IEEE) and the European Telecommunication Standards Institute, have issued technology-specific standards including security guidelines (K. Zhao & Ge, 2013). These standardization efforts have also brought up other initiatives for unified architecture and modeling, such as the Reference Architecture Model Industrie 4.0 (RAMI 4.0) (Adolphs et al., 2015), the industrial Internet reference architecture (Consortium et al., 2015), and the Internet of Things-Architecture (Heu, Heu, Cea, & Stefa, 2013). Figure 2 illustrates the IoT concepts and security approaches from different bodies of standard organizations. Each one of these documents is intended for different audiences with different focus of the IoT areas, and corresponding conceptual approaches to secure the IoT systems.

Architecture and model implementation helps IoT developers to focus and structure their efforts on users' requirements, which include connectivity, device management, data collection and analysis, scalability, and security. Nevertheless, additional

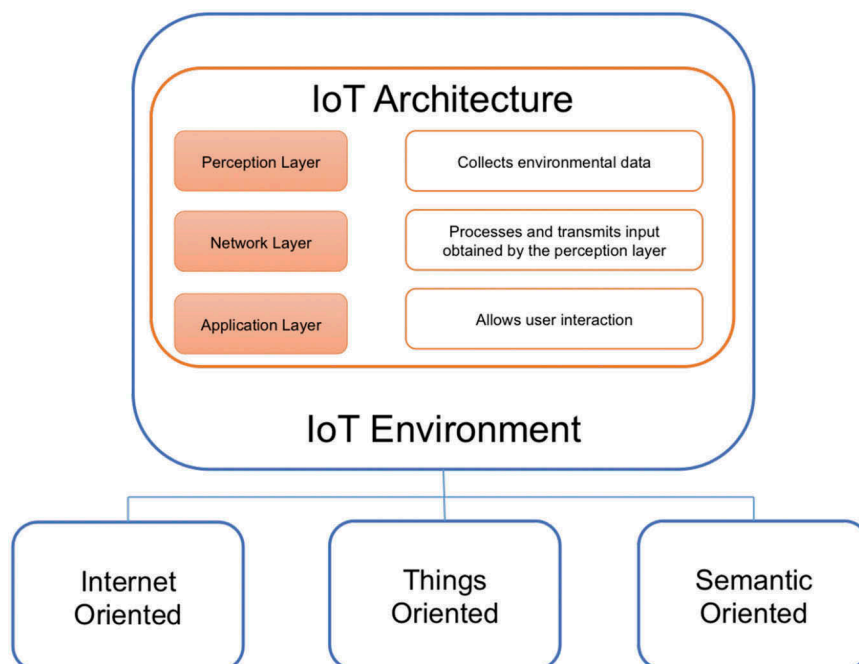
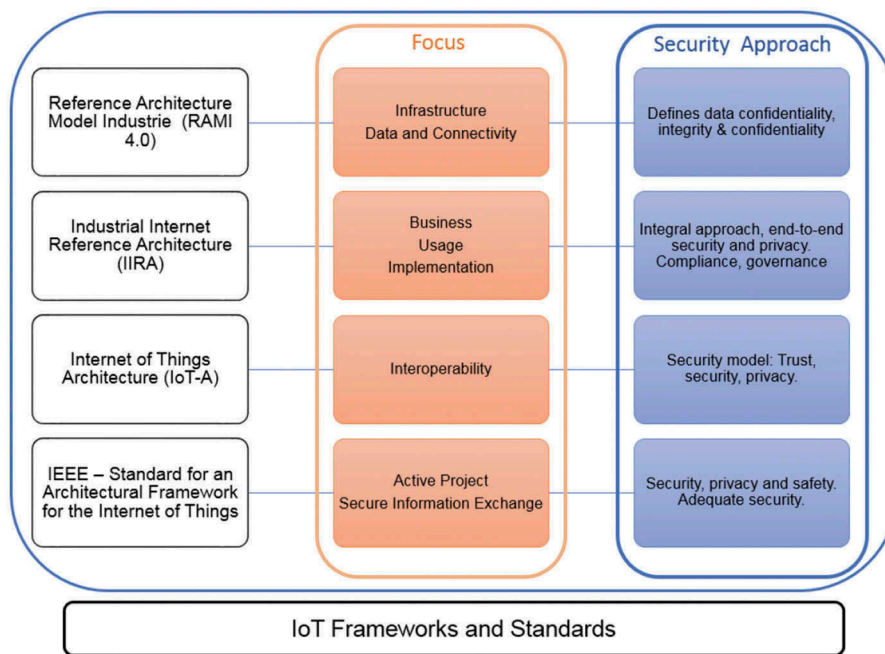


Figure 1. Current IoT architecture and environment.



**Figure 2.** Current IoT frameworks and standards.

unification attempts are needed for simplification and taking security communications as the main actor and enabler of IoT initiatives (Weyrich & Ebert, 2016). Besides the industrial domain, the scientific community has been a main contributor to the standardization of IoT protocols and technology as well (Atzori et al., 2010). The author of Weber (2015) advocated for the need of a security-based architecture, which is lacking at the moment, where resiliency, authentication access restriction, and privacy are important requirements for the future. Also, the authors of Khan, Khan, Zaheer, and Khan (2012) supported a reliable architecture that address security and service requests. From a different perspective, the authors of Ning and Wang (2011) promoted the importance of robust and reliable standards to conduct shielded IoT architectures, which is also required by the security community.

### Vulnerability landscape

More and more IoT security incidents were discovered in recent years and most of them provoked debates from technological, ethical, and privacy perspectives. In October 2016, the massive distributed denial of service (DDoS) attack on Dyn – a company that controls much of the Internet’s domain name system infrastructure – by a botnet

army of IoT infected devices, has turned on the alarms on the consequences of faulty IoT protections and poor standards (on Security, 2016). This accentuates the need for additional research on the IoT security domain. Nevertheless, the number of publications addressing security issues and concerns for the expanding IoT has not fostered the same attention to scientists in the community, even though the number of publications for IoT technologies and applications has grown exponentially during the last 5 years (of Science Thomson Reuters, n.d.). Figure 3 shows a basic comparison of the number of publications for both subjects.

In spite of the issues presented above, there are some important discussions taking place between experts regarding the baseline of securing IoT systems. For instance, according to Borgia (2014), IoT devices demand the following set of security requirements in order to be considered as secure:

- Secure authentication
- Secure bootstrapping and transmission of data
- Security of IoT data
- Secure access to data by authorized persons

Weber (2010), determined similar security requirements for the IoT, which include: (a) attack resiliency, (b) data authentication, (c) access control, and finally

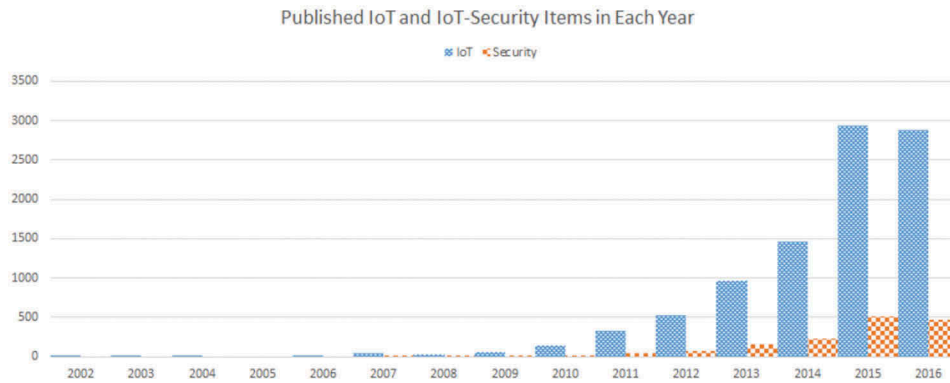


Figure 3. Number of publications for IoT and IoT security-related articles. Source: Web of Science.

demand (d) client privacy. Also, K. Zhao and Ge (2013) proposed security requirements to protect IoT data transmission, which include the following: (a) key management, (b) appropriate secret key algorithms, (c) secure routing protocols, (d) intrusion detection technology, (e) authentication and access control, and (f) physical security design.

For Zafari, Papapanagiotou, and Christidis (2015, 2016), the two main security-related issues have to do with data integrity and authentication. At the moment, the security and privacy requirements face serious challenges since current technologies do not offer feasible and comprehensive solutions applicable to the nature of the IoT. The unique scalability and

distribution properties of the IoT call for flexible and innovative security frameworks that can close the existing gaps and reduce the risk associated with the use of embedded computing devices. The energy-efficient principle as well as the low computing properties of IoT devices are antagonistic to the essence of cryptography algorithms of current security protocols, determined as the “security processing gap” according to Ukil, Sen, and Koilakonda (2011). IoT devices are also exposed to physical tampering, war driving, malicious software, and side-channel attacks (Ukil et al., 2011).

Security problems of the IoT need to be understood in order to find an appropriate solution (Figure 4).

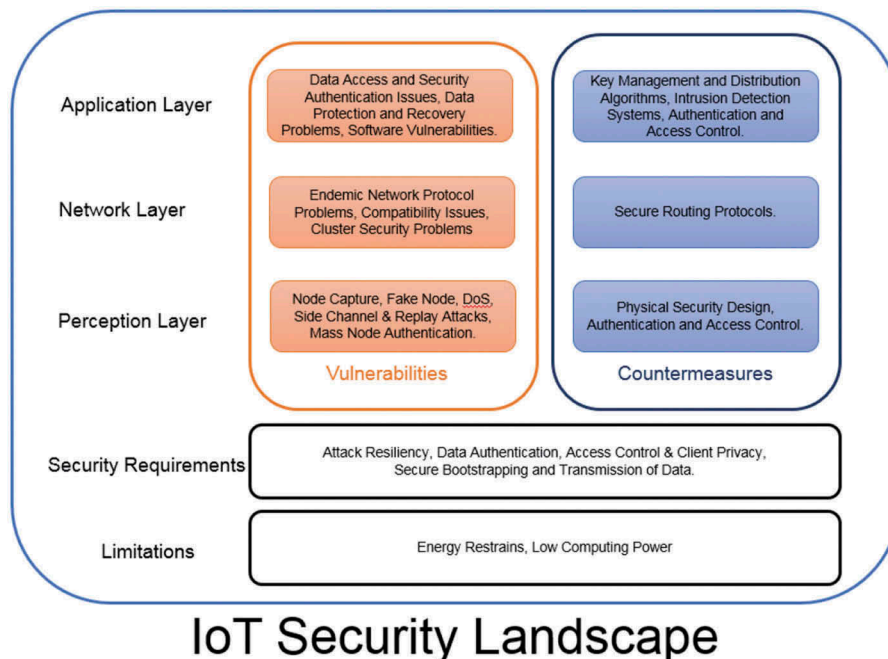


Figure 4. Internet of things security landscape.

The vulnerability landscape can be scrutinized from an architectural perspective. The perception, network, and application layers each presents security problems of their own but the security of IoT needs to be addressed as a whole. In Section IV, these layers are discussed in detail. Additionally, some other issues arise when the IoT platform is looked from a different technical perspective. For instance, Fernandes, Jung, and Prakash (2016) stated that 55% of Samsung-owned SmartThings development platform applications are over-privileged and therefore present important security risks.

### Enabling technologies and protocols

The IoT may be powered by different technologies with dissimilar properties for distinctive applications. However, those technologies also bring up some security issues that need to be addressed based on the capabilities and constrains that IoT devices offer at each IoT layer. This paper presents the following security concerns based on the IoT threat model presented by Atamli and Martin (2014), and specifically related to the external adversary entity. The authors of Atamli and Martin (2014, p. 38) defined external adversary as:

An outside entity that is not part of the system and has no authorized access to it. An adversary would try to gain information about the user of the system for malicious purposes such as causing financial damage and undermining the users credibility. Also, causing malfunction to the system by manipulating the sensing data.

### Perception layer

The perception layer is composed of physical elements of the IoT system. It comprehends sensors, transmitters, and its interaction with the outside world. It interfaces with the environment, which may include other IoT devices, and transmits it to the above layers for processing. Table 1 includes additional perception layer technologies.

### Wireless sensor networks

The authors in Boyle and Newe (2008, p.65) defined wireless sensor networks (WSN) “as a group of independent nodes communicating wirelessly offer limited frequency and bandwidth”. The success of WSN

often requires a massive sensor deployment and strict coordination. The limitations of WSN include “power management, network discovery, control and routing, collaborative signal and information processing, tasking and queering, and security”. According to Gubbi et al. (2013), the WSN network module includes the following components:

- a. Hardware
- b. Communication stack
- c. Middleware
- d. Secure data aggregation

Similar to active radio frequency identification (RFID) technology, the data collected by the sensor nodes are shared among them or by a centralized system for analytic purposes (Gubbi et al., 2013).

A WSN is composed of the following elements:

- a. Sensor
- b. Micro-controller
- c. Memory
- d. Radio transceiver
- e. Battery

A WSN consists of a centralize base station that controls a multi-hub relay system that connects the source nodes and the base (Borgohain, Kumar, & Sanyal, 2015). WSNs, as well as other network applications, require measures against common attacks including but not limited to denial of service (DoS), traffic analysis, node replication (Sybil attack), general confidentiality concerns, black hole routing attacks, and physical damage or unauthorized manipulation (Boyle & Newe, 2008). Boyle and Newe, (2008, p.66) also mentioned the necessity of a “common communication protocol” in order to find a feasible solution for system protection at the application level which includes IEEE 802.15.4 Security, Zigbee and Tiny OS protocols. Security requirements of WSN nodes are listed as follows:

- Data confidentiality
- Integrity
- Freshness
- Availability
- Organization autonomy
- Authentication



**Table 1.** Additional perception layer protocols.

Protocol	Security flaws	Countermeasures
<i>Radio frequency identification (RFID)</i>	<ul style="list-style-type: none"> <li>- Attacks on authenticity</li> <li>- Attacks on confidentiality</li> <li>- Attacks on availability</li> <li>- Privacy concerns</li> <li>- Physical and traffic analysis attacks (Henrici &amp; Mu"ller, 2004)</li> <li>- Cryptographic keys bruteforcing</li> <li>- Fault induction timing attacks</li> <li>- Power analysis attacks (Weis, Sarma, Rivest, &amp; Engels, 2004)</li> </ul>	<ul style="list-style-type: none"> <li>- Access control</li> <li>- Data encryption</li> <li>- IPSec protocol</li> <li>- Cryptography technology scheme (K. Zhao &amp; Ge, 2013)</li> <li>- Blocker tags(Henrici &amp; Mu"ller, 2004)</li> </ul>
802.11	<ul style="list-style-type: none"> <li>- Passive attacks (Djenouri, Khelladi, &amp; Badache, 2005)</li> <li>- Jamming and scrambling (Naeem &amp; Loo, 2009)</li> </ul>	<ul style="list-style-type: none"> <li>- Implementation of 802.11ah (Status of project ieee 802.11ah, n.d.)</li> </ul>
<i>Long-term evolution (LTE/LTE Advanced)</i>	<ul style="list-style-type: none"> <li>- Passive and active attacks</li> <li>- User tracking</li> <li>- Impersonation</li> <li>- False reporting of location</li> <li>- Exposure</li> <li>- DoS</li> <li>- DDoS (Bilogrevic, Jadliwala, &amp; Hubaux, 2010)</li> </ul>	<ul style="list-style-type: none"> <li>- Use of cryptographic tools</li> <li>- Implementation of adaptable schemes for identifiable information (Bilogrevic et al., 2010)</li> </ul>
<i>WiMax</i>	<ul style="list-style-type: none"> <li>- Jamming</li> <li>- DoS</li> <li>- Network mapping</li> <li>- Eavesdropping (Hasan &amp; Qadeer, 2009)</li> <li>- Man-in-the-middle attacks</li> <li>- Flawed authentication</li> <li>- Resource limitation (Rengaraju, Lung, Qu, &amp; Srinivasan, 2009)</li> </ul>	<ul style="list-style-type: none"> <li>- Additional schemes for authentication and key distribution (Huang &amp; Chang, 2008)</li> </ul>
<i>Near field communications (NFC)</i>	<ul style="list-style-type: none"> <li>- DoS</li> <li>- Unencrypted traffic (Curran, Millar, &amp; Mc Garvey, 2012)</li> <li>- Eavesdropping</li> <li>- Tag modification (Eun, Lee, &amp; Oh, 2013)</li> </ul>	<ul style="list-style-type: none"> <li>- Model based on random public keys by trusted service manager (Eun et al., 2013)</li> </ul>
<i>Bluetooth</i>	<ul style="list-style-type: none"> <li>- Optional or weak encryption</li> <li>- Non-secure default settings</li> <li>- Weak PIN usage</li> <li>- Insecure unit keys</li> <li>- Flawed integrity protection</li> <li>- Predictable number generator</li> <li>- Prone to man-in-the-middle attacks</li> <li>- Data corruption</li> <li>- DoS (Oka, Furue, Langenhop, &amp; Nishimura, 2014) (Bayram, Michailidis, Papapanagiotou, &amp; Devetsikiotis, 2013)</li> <li>- Privacy concerns (Zafari &amp; Papapanagiotou, 2015) (Zafari, Papapanagiotou, Devetsikiotis, &amp; Hacker, 2017)</li> </ul>	<ul style="list-style-type: none"> <li>- Use of pseudo-random frequency hopping</li> <li>- Restricted authentication</li> <li>- Encryption</li> <li>- User education (Bouhenguel, Mahgoub, &amp; Ilyas, 2008)</li> </ul>
<i>ZigBee</i>	<ul style="list-style-type: none"> <li>- Traffic sniffing</li> <li>- Packet decoding</li> <li>- Data manipulation</li> <li>- Physical security</li> <li>- Key sniffing attacks (Vidgren, Haataja, Patino-Andres, Ramirez-Sanchis, &amp; Toivanen, 2013)</li> </ul>	<ul style="list-style-type: none"> <li>- ZigBee trust center (Z. Alliance, 2006)</li> <li>- Z-Wave Alliance framework (Trends, n.d.) (Z.-W. Alliance, n.d.)</li> </ul>
<i>Ultra-Wideband</i>	<ul style="list-style-type: none"> <li>- Comparatively secure (Ullah, Ali, Hussain, &amp; Kwak, 2009)</li> </ul>	

WSNs vulnerabilities, according to Borgohain et al. (2015), can be categorized as the following: (a) attacks on secrecy and authentication, (b) silent attacks on service integrity, and (c) attacks on network availability. Availability attacks (DoS) against WSN devices can occur on different layers of the network including DoS attacks on the physical layer (jamming, node tampering), DoS attacks on the link layer (collision, unfairness, battery exhaustion), DoS attacks on the network layer (spoofing, hello flood, homing, selective forwarding, sybil, wormhole,

acknowledgement flooding), DoS attacks on the transport layer (flooding, de-synchronization), and DoS attacks on the application layer (traffic congestion generation). Attacks on WSN can further be classified on to one of the following categories: (a) external, (b) internal, (c) passive, (d) active, (e) mote-class, (f) laptop class, (g) interruption, (h) interception, (i) modification, (j) fabrication, (k) host-based, and (l) network-based (Borgohain et al., 2015).

Authors of Sicari, Rizzardi, Grieco, and Coen-Porisini (2015) affirmed that work has been done

to secure WSN. However, some questioning has been arising. The questioning involves adaptability to the heterogeneous properties of IoT devices, network layer security management determination, feasibility of re-utilization of existing encryption protocols, and end-to-end integrity verification. The authors also mentioned some additional efforts that include lightweight encryption methods, such as elliptic curve cryptography (ECC), to protect privacy and avoid counterfeiting attempts, which require additional standardization efforts to meet confidentiality expectations of the IoT infrastructure.

WSN security concerns can be addressed, to some degree, by the use of authentication methods through public key infrastructure (PKI) to prevent unauthorized access and mitigate DoS risks (Medaglia & Serbanati, 2010).

According to Boyle and Newe (2008), node authentication can solve most of the problems that may be caused by unauthorized uses. Some of the authentication methods discussed take into account Security Protocols for Sensor Networks (SPINS) composed of secure network encryption protocol, micro-Tesla, TINYSEC, localized encryption and authentication protocol (LEAP/LEAP+), and Zigbee.

### ***IPv6 low power personal area networks (6LoWPAN)***

Since the conceptualization of IoT technologies, research has inclined to select IPv6 as the choice for wireless communication. 6LoWPAN communication standard applies IPv6 to the PHY and MAC layer of the existing 802.15 standard. According to Sheng et al. (2013), the key features of IPv6 for the IoT are universality, extensibility, and stability. It has special characteristics such as small packet size, low-bandwidth, and large number of devices. According to Park et al. (2011), the security challenges for a 6LoWPAN network are (a) minimizing resource consumption and maximizing security performance, (b) 6LoWPAN deployment enables link attacks ranging from passive eavesdropping to active interfering, (c) in-network processing involves intermediate nodes in end-to-end information transfer, (d) 6LoWPAN communication characteristics render traditional wired-based security schemes unsuitable. 6LoWPAN is

susceptible to various attacks, the list of threats based on ISO OSI layers: (a) 6LoWPAN devices are vulnerable to physical attacks like node tampering, destruction, and masking. Several types of DoS attacks can be triggered at different layers. At physical layer, jamming and node tampering. (b) Attacks at MAC layer include collision, battery exhaustion, and unfairness. (c) At network layer, 6LoWPAN is vulnerable to spoofing attacks as well as altered, or replayed routing information attacks, selective forwarding, sinkhole attack, Sybil attack, wormhole attack, and neighbor discovery attacks. (d) An attack against the transport layer is performed by half open, half closed Transmission Control Protocol (TCP) segment. The attacker continuously forges messages carrying sequence numbers or control flags. This will cause the endpoints to request retransmission of missed frames leading to DoS attack due to large amount of traffic. A secure 6LoWPAN protocol should provide:

- Data confidentiality
- Data authentication
- Data integrity
- Data freshness
- Availability
- Robustness
- Resiliency
- Resistance
- Energy efficiency
- Assurance

To ensure maximum security 6LoWPAN should employ secure bootstrapping mechanisms, Secure Neighbor Discovery protocol extended to support ECC encryption algorithm which uses smaller-packet sizes compared to RSA and secure key management algorithms engineered to suit the specific characteristics of 6LoWPAN.

### ***Middleware***

The challenges presented between each one of the architectural components of embedded systems, these components are not necessarily compatible or able to communicate or interact with each other. The middleware is the interaction enabler between devices or other layers and applications, it has been adopted by the IoT to bond different



components and make them work as part of the same architecture. Middleware in the IoT is used as well to interact with “cloud technologies, centralized overlays, or peer to peer systems” (Sicari et al., 2015, p.146). Evidently, the attack surface increases the demand for more comprehensive IoT security, moreover, the lack of standardized approaches do not permit a comprehensive response to all IoT security and privacy requirements. Services such as context-awareness may risk personal privacy as critical user information may be disclosed by malicious parties (Razzaque, Milojevic-Jevric, Palade, & Clarke, 2016). The authors of Razzaque et al., (2016, p.76) propose seven categories for discussion based on design principles, shown in Table 2.

### **Application layer**

The application layer is responsible of making sense out of the data collected and transmitted for the other IoT layers. The application layer filters, processes, and presents the data to the user or to other platforms, it provides the intelligence to the system. Therefore, this layer is expected to meet high security requirements (Jing, Vasilakos, Wan, Lu, & Qiu, 2014). The more common security issues of the layer relate to access control, privacy protection, user authorization, data integrity, availability, reliability, and privacy (Jing et al., 2014). The authors of Suo, Wan, Zou, and Liu (2012, p. 649) indicate that “the data sharing capabilities provided by this layer brings up security concerns of data privacy, access control and disclosure of information”. Moreover, over recent years, the application layer has caught the attention of security researchers and business owners as cloud computing has taken over many of the current implementation for IoT applications. Risk estimation cannot be overseen as cloud platforms may differ on the way the data are handled for encryption, data monitoring, and back up (Jing et al., 2014). According to Suo et al. (2012), authentication and key agreement over heterogeneous networks are fundamental to find a solution for security issues at this layer. Nevertheless, we believe that current technologies that run on the application

layer need to be discussed on detail based on the intrinsic characteristics of each one of them.

### **Message queue telemetry transport (MQTT)**

The characteristics of the various devices used in IoT are such that they lack the capability to handle high-level protocols like HTTP. Researchers are more inclined to develop light-weight protocols that suit the specific characteristics of IoT devices. The MQTT proposed by Stanford-Clark (2014) in 1999 is a light-weight protocol designed for constrained devices and low-bandwidth, high-latency, or unreliable networks. The present implementation of MQTT provides support for only identity, authentication, and authorization policies. The basic approaches used to support these policies are by using a username/password pair, which is set by the client, for identification or by authentication performed by the MQTT server via client certificate validation through the Secure Sockets Layer (SSL) protocol. The MQTT server identifies itself with its IP address and digital certificate. The MQTT communication uses TCP as transport layer protocol. By itself the MQTT protocol does not provide encrypted communication. Authorization is also not part of MQTT protocol. Authorization is provided by MQTT servers. MQTT authorization rules control which client can connect to the server and what topics a client can publish or subscribe to. According to Neisse, Steri, and Baldini (2014), the security controls provided by MQTT are not sufficient for the IoT network. IoT networks require “data anonymization, obfuscation or dynamic context-based policies that should be dynamically evaluated for each message forwarded by the broker” (Neisse et al., 2014, p. 1). Neisse et al. (2014) implement a solution for the enforcement of security at MQTT layer which is a Model-based Security Toolkit called SecKit. It addresses the privacy and data protection requirement. For secure communication, security mechanisms have to be adopted over existing MQTT protocol. M. Singh, Rajan, Shivraj, & Balamuralidhar (2015) propose a new security solution for MQTT (Secure MQTT or Secure Message Telemetry Transport (SMQTT) that replaces the use of SSL/TLS certificates, which are not necessarily viable in all IoT implementations, the solution runs over lightweight attribute-based encryption over elliptic curves.

**Table 2.** Middleware applications and security features.

Design categories	Applications w/ security features	Applications w/o security features
<i>Event-based</i>	- HERMES (Pietzuch, 2004)(Confidentiality through X.509 and OASIS role memberships)	- EMMA - GREEN - RUNES - Steam. - MiSense - PSWave
<i>Service-oriented</i>	- HYDRA (Eisenhauer, Rosengren, & Antolin, 2010) - SOCRADES (Guinard, Trifa, Karnouskos, Spiess, & Savio, 2010) - UbiSOAP (Caporuscio, Raverdy, & Issarny, 2012) - KASOM (Corredor, Martínez, Familiar, & López, 2012) (Razzaque et al., 2016) (Authentication only) - Xively (Xively, n.d.) (Not for storage components) - Carriots (Carriots, n.d.) (Not for storage components)	- Tiny DDS (Razzaque et al., 2016) - Servilla (Fok, Roman, & Lu, 2012) - Echelon (Echelon, n.d.) (Razzaque et al., 2016) - SenseWrap - MUSIC - TinySOA - SensorMW - SENSEI - KASOM - CHOReOS - MOSDEN - WhereX (Razzaque et al., 2016)
<i>Virtual machine-based</i>	- Mate (Costa, Pereira, & Serodio, 2007)	- VM - Melele - MagnetOS - Squawk - Sensoware - DVM - DAViM - SwissQM - TinyReef (Razzaque et al., 2016)
<i>Agent-based</i>	- Ubiware (Nagy et al., 2009)	- Impala - Smart Messages - ActorNet - Agilla - UbiROAD - AFME - MAPS - MASPOT - TinyMAPS (Razzaque et al., 2016)
<i>Tuple-spaces</i>		- LIME (Murphy, Picco, & Roman, 2001) - TinyLIME (Curino et al., 2005) - TS-Mid (Lima, Rosa, & Marques, 2008) (Razzaque et al., 2016)
<i>Database-oriented</i>		- GSN (Aberer, Hauswirth, & Salehi, 2006) - HyCache (D. Zhao & Raicu, 2013) - TinyDB (of California Berkeley, n.d.) (Razzaque et al., 2016)
<i>Application specific</i>		IoT Security demands not satisfied integrally (Razzaque et al., 2016)

### ***Extensible messaging and presence protocol (XMPP)***

The XMPP is an application profile of the Extensible Markup Language (XML) that enables the near-real-time exchange of structured and extensible data between any two or more network entities. The core features of XMPP provide the building blocks for different types of near-real-time applications, which can be layered on top of the core by sending application-specific data qualified by particular XML namespaces (Saint-Andre, 2011). XMPP architecture is defined by a distributed network of clients and servers. The recommended ordering of layers in

XMPP described in Saint-Andre (2011), in order to ensure security, is to have TCP, followed by TLS, SASL, and then XMPP. Using XMPP over TLS provides confidentiality and integrity to data which is in motion over the network. Unless the network is protected with TLS, it is open to attacks. But the XMPP protocol does not provide end-to-end security. The data are processed in cleartext on the sender's and the receiver's servers. It is also unprotected when it is sent from the sender's to the receiver's server, or sent from receiver's server to receiver's client. Systems using XMPP as the enabling

**Table 3.** Comparison between most cited publications for IoT security according to the Web of Science database.

	(Gubbi et al., 2013)	(Miorandi et al., 2012)	(Bandyopadhyay et al., 2010)	(Roman et al., 2011)	(Zhou & Chao, 2011)	(Hong et al., 2010)	(Zuehlke, 2010)	(Sarma & Gira'o, 2009)	(Roman et al., 2011)	(Yan, Zhang, & Vasilakos, 2014)
Enabling technologies										
WSN	✓			✓		✓			✓	✓
RFID	✓			✓			✓		✓	✓
Ultra-Wideband										
802.11										
LTE/LTE advanced										
NFC			✓							
Bluetooth										
6LoWPAN						✓			✓	✓
ZigBee						✓				
MQTT										
XMPP										
Blockchain										
Security triad										
Confidentiality	✓	✓	✓	✓	✓	✓			✓	✓
Integrity	✓	✓		✓	✓	✓			✓	✓
Availability	✓	✓	✓	✓	✓		✓		✓	✓
Authentication	✓	✓	✓	✓	✓		✓	✓	✓	✓
Accounting								✓	✓	✓
Privacy	✓	✓	✓	✓	✓		✓	✓	✓	✓

technology must ensure that they use secure protocols along with XMPP. For authentication purposes, the servers and the clients should support Salted Challenge Response Authentication Mechanism (SCRAM). Using both TLS and SCRAM provides both confidentiality and authentication. Due to its capability of real-time message exchange, XMPP is a viable enabling technology for the IoT but XMPP has to be used in conjunction with the various security protocols to ensure confidentiality, integrity, and authentication of the IoT system.

### **Blockchain**

Blockchain (Christidis & Devetsikiotis, 2016) was originally proposed in Bitcoin to solve the double spending problem in a cryptocurrency system. However, a blockchain can stand by itself and be applied in a distributed and trust-less environment without the need of third party authentication or management. In a nutshell, a blockchain is a back-ordered hash list that is publicly shared in a peer-to-peer network. Usually, each member in the blockchain system is addressable by the hash value of its public key. When a new transaction occurs, the owner of the transaction can prove the authenticity of the record (i.e. block) by encrypting the hash value of the record using its private key. The newly formed block is then appended to the existing blockchain and point to the previous block. Supported by the cryptographic properties of hash and asymmetric encryptions, a blockchain can therefore ensure each block is immutable and transaction is verifiable. Blockchains has recently received a lot of attentions in the field of IoT. Researchers and practitioners believe blockchain is one of the key technologies that can securely enable smart contracts among the things. That is, smart devices can interact and transact with each other autonomously without human interventions. Though it is possible to implement blockchains in a public network, the computing overhead of providing proof of work (mining) may overwhelm the limited computing resources in an IoT network. If on the other hand, participating members in a blockchain network are not completely trust-less, simple techniques, such as white listing, can be leveraged to reduce the burden of mining and make blockchains much more desirable in real world practice. It should be noted that,

blockchains offer only pseudo anonymity: it is possible for adversaries to make inferences about who owns what public keys. If privacy is a major concern in an IoT system, additional mechanism must be designed and implemented to prevent the owners of the smart devices being identified.

### **Confidentiality, integrity, availability, and privacy concerns for IOT systems**

An upcoming global network of “things” brings challenges regarding security and privacy. Confidentiality, integrity, and availability become paramount when exchanging data between IoT devices. The intelligence and autonomy of these devices demand further responsibility when protecting against device corruption and its influence in the network (Mayer, 2009). Different cryptographic and process-based solutions are available to assure and to provision confidentiality, integrity, and availability. Nevertheless, IoT systems demand not only these services, but also need to focus on how these solutions are executed and optimized (Heer et al., 2011a; Singla, Mudgerikar, Papapanagiotou, & Yavuz, 2015b; Singla, Mudgerikar, Papapanagiotou, & Yavuz, 2015a; Yavuz, Mudgerikar, Singla, Papapanagiotou, & Bertino, 2017). It is, then, necessary to analyze the IoT entire platform under fundamental notions of security that can add perspective to security researchers and advocates on the main properties that a secure IoT solution must present.

The IoT relies heavily on wireless networks which are known to be vulnerable to all type of intrusions including unauthorized router access, faulty configurations, jamming, man-in-the-middle attacks, interference, spoofing, DoS attacks, brute-force attacks, traffic injections, etc. (Acharya & Asha, 2008). According to Gubbi et al. (2013), security is a main concern for large networks, therefore, IoT physical components are vulnerable to availability, confidentiality, and integrity attacks. The “first line of defense” (Gubbi et al., 2013, p. 14) is the application of cryptographic features. Encryption schemes protect confidentiality as message authentication codes assure integrity as well as authenticity. Former WSN implementations, according to Christin, Reinhardt, Mogre, and Steinmetz

(2009), used to deal with attack models that required physical access to the nodes. Eventually, after opening WSNs to the Internet the threat model changed as attackers can reach WSNs ubiquitously where sensor nodes are the most vulnerable due to scarce computational resources. According to Uckelmann, Harrison, & Michahelles (2011), in order to enable massive adoption of IoT devices; security, including confidentiality, integrity, availability, and privacy issues must be addressed in order to make them trustworthy to the public. Uckelmann et al. (2011) suggested as well that there should exist different security levels since the requirements are not the same between devices. User privacy and integrity can also be endangered from the lack of data confidentiality and integrity. Unauthorized access of sensor data could interfere with the proper functioning of the system, as well as unauthorized access and control (Medaglia & Serbanati, 2010).

IEEE standard 802.15.4, which provides guidelines to protect physical and medium access control layers, may be used as an instrument to add security features that sum up confidentiality, integrity, and availability properties to the system (Medaglia & Serbanati, 2010). The Internet Draft ID-Tsao (Tsao, Alexander, Dohler, Daza, & Lozano, 2011) signaled a high-level presentation of the existing threats and security countermeasures in terms of the security triad. Garcia-Morchon, Hummen, Kumar, Struik and Keoh (2012) indicated a potential limitation of the framework based on the non-differentiation arguments and layer 3-only analysis.

### **Confidentiality**

Miorandi, Sicari, De Pellegrini, and Chlamtac (2012, p.1505) defined data confidentiality as a “fundamental issue” for IoT solutions, “particularly relevant in the business context”. Miorandi et al. (2012) also indicated that current data confidentiality solutions may not be applicable as is due to two main limitations: Amount of data generated and the effectiveness in the control of access to data of dynamic data streams. The authors in Miorandi et al. (2012) also mentioned proper identity management (IdM) as a key factor to

assure data confidentiality. Some IoT devices need to handle data that requires to be classified as confidential. Confidentiality, of the communications channel, can be obtained through encryption schemes. Current symmetric and asymmetric algorithms should be analyzed before implemented based on the application, capability, and the criticality of the IoT system as stated by Alam, Chowdhury, and Noll (2011).

Wireless communications of things may be vulnerable to eavesdropping attacks that may compromise the confidentiality of the communication which could impact the node or the network as a whole (Garcia-Morchon et al., 2012). Suo et al. (2012) emphasized on the importance of confidentiality research and the inherent challenges attached to it. Suo et al. (2012) also indicated the significance of authenticity and the integrity of data groundwork as well. The confidentiality needed for a sensor data, according to Suo et al. (2012), is not as important as the integrity and authenticity since the attacker may obtain the same values just by placing a rogue sensor next to the legitimate one. Mayer (2009) stated that the major confidentiality sensitivity, in the context of IoT, resides in the communication, storage, localization/tracking, and identification. On the other hand, sensors, actuators, devices, and processing topics are not as sensitive as the one listed in the first place. According to Mineraud, Mazhelis, Su, and Tarkoma (2015, p. 4), IoT solutions must use security mechanisms that permit, based on the end-user decision, access to a “predefined set of resources”, also called data ownership. It is needed then a differentiation for the security requirements of things based on criticality. Heer et al. (2011b) indicated the importance on the difference for each of the IoT layers, the link layer, the network layer, and the application layer. Current IoT technologies manage data security processes, including key management, which places a burden on IoT resources that may diminish IoT capabilities and increase risk (J. Singh, Pasquier, Bacon, Ko, & Eysers, 2015). Babar, Stango, Prasad, Sen, and Prasad (2011) proposed the use of lightweight cryptographic algorithms so that the resource-limited IoT devices, especially for processing and storage capabilities, can provide data protection and,



therefore, confidentiality. Datagram transport layer security (DTLS) may be used as a solution to confidentiality problems by providing end-to-end security for the application layer. DTLS properties may also reduce the impact and the cost of resources of constrained devices compared to other solutions (Garcia-Morchon et al., 2012). In order to protect data and communication confidentiality, some cloud-based solutions establish secure channels based on cryptographic features relying on PKI. Information flow control is noted as another solution to protect IoT data sharing utilizing a cloud-based platform that protects critical information as described by Singh, Pasquier, et al., (2015).

According to Bandyopadhyay and Sen (2011), privacy of people and business confidentiality are two major issues to be addressed for the IoT. Standard encryption schemes may solve the problem. In addition, energy consumption and processing resources for encryption, decryption, and key distribution must be effective and efficient when evaluating a valid IoT solution. Confidentiality and privacy are usually tied together, according to Weber (2015, p. 622), “Privacy as confidentiality represents solutions for anonymizing the collected data (including communications) and minimizing the collection of data”. Weber (2015) also suggested that anonymous communication, such as hiding location, identity, time, frequency, and volume details, as well as communication context is necessary to entirely protect traffic data from unauthorized access Weber (2015) also stated that in order to increase confidentiality levels it is important to apply privacy-base designs and privacy-enhancing technologies to make it possible.

Confidentiality also deals with government regulations and laws that demand data protection and confidentiality (Singh, Pasquier, et al., 2015). Coetzee and Eksteen (2011) stated that trust is fundamental for users of the IoT as the information shared by the things and the users will not be compromised. To do so, the principles of data confidentiality and security itself must be preserved. According to Miorandi et al. (2012), data confidentiality, privacy, and trust are key factors that can leverage the widespread adoption of IoT technologies and applications.

## **Integrity**

IoT integrity deals with physical failures and damages at first sight. Integrity protection includes preservation against sabotage and the use of counterfeit units or components (Sadeghi, Wachsmann, & Waidner, 2015). Another critical factor that influences data integrity is the robustness and fault tolerance capabilities of the IoT System (Miorandi et al., 2012). Sensor networks, such as RFID solutions, face also other issues that limit their capability to overcome integrity problems as many of their components spend most of the time without being attended. Attackers can either modify the data while it is stored in the node or when it travels through the network. Read and write protections as well as authentication methods are common solutions to these issues. Data integrity is also ensured by password-based solutions, which brings into account the shortcomings of password protection, such as vulnerabilities related to password length and randomness. Also, the resources found in common IoT systems do not support typical cryptographic solutions because of the limited resources available (Atzori et al., 2010).

Integrity for the IoT not only is required to be guarded from external sources but also for internal processes, such as service integrity. Operating systems rigid process separation, known as multilevel security (MLS), helps devices to avoid unauthorized modification from code running with high privileges. Nevertheless, MLS approaches have not been deployed widely as in some cases can be considered as expensive as well as not compatible with other IoT software. Other approaches to guarantee integrity use hash values which are stored externally to avoid compromises (Fongen, 2012). Hardware solutions have also been proposed for integrity purposes, a challenge-based solution is mentioned in Fongen (2012) by the use of symmetric or asymmetric keys known as trusted platform module.

Process integrity is also required by IoT devices. It relies on the device, communication, and algorithm implementation integrity. The processing data correctness is highly desired to perform data processing for higher services and data correlation (Mayer, 2009). Software integrity relies mostly on hardware isolation of critical code and data from other, less

relevant, internal components and it can be hardware-enforced. SMART, SPM, SANCUS, and Trustlite are some solution examples applied to devices with limited capabilities in terms of processing, power, and battery life (Sadeghi et al., 2015). Nevertheless, hardware-based attacks, such as fault attacks, can compromise the integrity if the system does not have protections in place, i.e. perturbation sensors (Van Tilborg & Jajodia, 2014). Integrity verification for software configuration, called attestation, prevents malicious modifications and it is usually performed through secure hardware. However, IoT devices are forced to depend on software attestation which is based on “strong assumptions” that are not easy to accomplish in practice. Instead, low-end embedded devices may use “swarm attestation” that allows software integrity verification collectively from multiple devices or “provers” (Sadeghi et al., 2015).

Authentication schemes used in the IoT not only try to assure the identity of an object but also attempts to ensure its integrity. Authentication, through IdM provides resource control and helps to deliver auditing, accounting, and access control as well. Nevertheless, the implementation of IdM presents some challenges when deployed in an IoT infrastructure after facing scalability, capability, and management issues (Fongen, 2012). Standardized procedures are also important for ensuring integrity and quality as well. A common scheme permits the process development to satisfy data trustworthiness and traceability needs. Extensive collaboration between different IoT institutions and alliances is fundamental (Miorandi et al., 2012).

### **Availability**

Usual information networks, according to Suo et al. (2012, p. 648), need to guarantee “identification, confidentiality, integrity, and undeniability”. Nevertheless, IoT networks can potentially be utilized in “crucial areas of national economy”, which need as well to pay special attention to availability and dependability. According to Kasinathan, Pastrone, Spirito, and Vinkovits (2013, p. 601), for information networks, device availability is the “most important factor”. IoT availability requirements, as specified by Roman, Zhou, and Lopez (2013), are highly tied to reliability requirements.

IoT systems need to display sufficient resiliency to sustain availability under desired levels as well as they need to guarantee a certain level of performance requested by their applications. Availability may also refer to ubiquitous requirements, Al-Fuqaha, Guizani, Mohammadi, Aledhari, and Ayyash (2015) proposed that in order for IoT devices to reach their full potential they will need to address the availability requirements, which is listed as a key challenge to be addressed for the IoT. Al-Fuqaha et al. (2015, p. 2362) also stated that the availability of the IoT networks should be performed in hardware and software so they can cope with user requirements. “Availability of software refers to the ability of the IoT applications to provide services for everyone at different places simultaneously. Hardware availability refers to the existence of devices all the time that are comparable with the IoT functionality and protocols”.

According to Sheng et al. (2013), some constrained devices may face similar effects as a DoS attack from huge amount of legitimate clients’ requests that may hinder the services provided. Still, current Internet Engineering Task Force standardized communication protocols, such as Constrained Application Protocol, failed to provide solutions and, therefore, foster IoT network availability.

DoS attacks obstruct the communication between devices and prevent them for accessing network resources. According to Kasinathan et al. (2013), DoS attacks are important security issues that need to be addressed. DoS attacks can be executed remotely with simple commands in combination with more sophisticated tools that may allow the execution of DDoS attacks as well. DoS attacks against IoT systems, as exposed by Roman et al. (2013), not only deal with traditional vectors, such as service provider resource and bandwidth exhaustion but also they can compromise data acquisition wireless communication from IoT nodes. Suo et al. (2012, p. 649) stated that DDoS are “particularly severe” for IoT systems constituted of vulnerable nodes from a network layer standpoint. Kasinathan et al. (2013) define the range of DoS attacks, from the simplest one, such as jamming attacks (the interference of radio signals), to sophisticated ones, such as elaborated DDoS. DoS and DDoS attacks not only can affect the availability of network resources or applications, but also may cause energy

dissipation issues, which is critical for constrained devices (Misra, Krishna, Agarwal, Saxena, & Obaidat, 2011). Physical damage, as stated by Roman et al. (2013), can also be considered a DoS threat executed by less knowledgeable attackers to cripple IoT services by “things” destruction.

Misra et al. (2011) define DDoS attacks as the set of concurrent DoS attacks. Therefore, the authors suggest in their work, a service-oriented architecture as a DDoS prevention strategy for IoT systems. Traditional approaches to prevent DoS or DDoS attacks rely on heavy network traffic sampling, Misra et al. (2011) propose an optimized solution based on random sampling and sampling rate efficiency. Kasinathan et al. (2013) list various DoS defense techniques for WSN including Raymond and Midkiff (2008), Garcia-Morchon et al. (2012), and Heer et al. (2011b). Nevertheless, the authors stated that there is not an existing defense mechanism capable of ruling out DoS risks. DoS attack detection is very difficult to accomplish, according to Kasinathan et al. (2013), since the symptoms of such attacks may also make some services unavailable. Kasinathan et al. (2013), proposed an intrusion-detection-system-based solution for DoS attack detection. The solution objective is to detect DoS attacks in early stages before the disruption of normal network operations for 6LoWPAN solutions. The authors of Roman et al. (2013) suggested the implementation of distributed architectures instead of centralized approaches. One of the main advantages portrayed in the same work, is the improvement of availability properties in terms of service uptime as well as eliminating single points of failure. Suo et al. (2012) stressed on the importance of disaster recovering procedures to be placed after large-scale or elaborated DDoS attacks.

### Privacy

The significant growth that the IoT has shown during recent years has brought in several privacy concerns as data availability soars, sponsored by ubiquitous and pervasive properties of the IoT (Miorandi et al., 2012; Stankovic, 2014) and the fact that devices at the moment do not offer all the desired warranties. Sicari et al. (2015) called for protection of users’ personal information associated to their “movements, habits and interactions” (Sicari et al., 2015, p. 151). Faulty

provisioning of data confidentiality and integrity could influence user privacy as malicious parties could access sensitive data without any authorization or consent (Medaglia & Serbanati, 2010; Atzori et al., 2010), harming as well the possibility for widespread adoption of IoT technologies (Atzori et al., 2010; Miorandi et al., 2012; Tan & Wang, 2010). Roman, Najera, and Lopez (2011) discuss worst-case scenarios and undesirable situations produced by “Big Brother-like entities” (Roman et al., 2011, p. 54) where data are collected and shared without user consent.

Vermesan and Friess (2013) distinguished issues and challenges that the IoT community needs to address in order to prevent privacy violation, which includes self-aware behavior of interconnected devices, data integrity, authentication, heterogeneity tolerance, efficient encryption techniques, secure cloud computing, data ownership and governance, as well as policy implementation and management. Roman et al. (2011) also proposed solutions to the IoT privacy problems. The first one is to provide “privacy by design” (Roman et al., 2011, p. 64) which advocates for users to have the tools to dynamically control the data collected, stored, and shared. User’s request should be correlated and evaluated to existing policies in order to make a decision whether to grant data access or not (Stankovic, 2014). Weber (2015) introduced transparency as a privacy solution because this enables the users to know the parties that manage and utilize the data collected by a IoT device. Stankovic (2014) proposed Data Management as a solution, composed by implementing differentiated policies and enforcing instruments. Stankovic (2014) discussed the necessity of data typification, ownership, access extent (minimum and maximum of data to be read), anonymity, and its viability. Atzori et al. (2010) proposed the implementation of opt-out features managed by individuals. This can be done by implementing an untrustworthy sensor network, which includes “right to silence of the chips” (Weber, 2010, p. 26), as well the interaction with a “privacy broker” (Lioudakis et al., 2007, p.966) that acts as a proxy between the user and the network. Tan and Wang (2010) stated that technological solutions are not enough to address the current privacy issues and calls for the consideration of economical and socio-ethical aspects of the IoT environment. Roman et al. (2013) supported the idea of revising the existing

privacy regulations for both private sector and public sector. In addition, users' awareness needs to be improved to comprehend how sensor-based devices collect, store, and share their information. However, it is not that simple to achieve user awareness. In addition, the distinction and classification between Personal Identifiable Information (PII), which needs to be protected by law, and non-identifiable information is still a challenge in the world of IoT (Peppet, 2014). Weber (2010) questioned whether IoT privacy regulations should be covered by governmental or by self-regulatory entities (current trend). Government regulations could be only applicable locally when the nature of IoT data transcends the jurisdiction boundaries. Nevertheless, government entities, such as the European Commission and the US Federal Communications Commission (Weber, 2015), have already called for recommendations in the deployment of sensor networks as well as the collaboration within the civil society stakeholders to create a privacy framework that works at different levels.

Privacy has become a fundamental aspect and a sought feature for any IoT system. The more data IoT devices handle the more important privacy becomes. Personal information, daily habits, medical conditions, business secrets, location data, etc. can be wrongfully accessed in an ill-protected IoT system. Financial, political, or even personal motivations can serve as a vehicle for nefarious actors to intrude IoT implementations. Such scenario could harm not only the affected users but also the IoT as a whole, as the trustworthiness on IoT plunges and general disappointment overcome the advantages IoT provides.

### **IoT security challenges and some solutions**

Different authors with different terminologies coincide on determining the architectural structure of the IoT. The perception, the network, and the application layer (middleware can be placed in between the last two layers) constitute what currently the IoT relay on, with each layer provides significant value to the whole system. These segmentation provide modularity and helps systems to escalate more efficiently. However, it also allows malicious entities, in this context external attackers under the threat model defined, to exploit vulnerabilities intrinsic to each one of the IoT layers. Each one of the IoT

components of the different layers can be run on top of separate technologies and, therefore, distinct weaknesses are found based on functionality and application. Such vulnerabilities have been exploited in a way that have compromised millions of IoT devices which have resulted in the perfect weapon to execute one of the most Internet-disruptive breakdowns in recent times. Even though security researchers have expressed their concern over the weaknesses of IoT systems, the intrinsic principle of energy efficiency as well as low computing power available on embedded devices are in some way antagonistic to the existing cryptography principles, that means a more challenging environment for the IoT and its community. Table 3 provides a comparison between the most cited publications for IoT Security according to the Web of Science database.

The IoT, then, needs a deeper discussion that strengthens its foundations toward a secure environment. In order to contribute to this purpose, the authors of this document consider that further analysis under the security triad (confidentiality, integrity, and availability) is necessary. Also, this work covers the privacy concerns that the ongoing soaring demand for IoT devices has brought along. Many IoT experts have raised their concerns on how "Big Brother-like" entities may collect and disclose users' data without consent and how technological and governance implementations may help to relieve the existing doubts. As stated, the situation of the IoT under a security perspective is concerning and proper analysis and consequent actions are required. The need for integral standards as well as for more hardware-friendly security implementations is now of common understanding. Policy is also a priority for user protection and manufacturer regulation in order to find a more fertile ground for IoT expansion.

### **Conclusion**

The current state of IoT reveals that there is still a significant work to be done in order to secure embedded computer devices. Even though the number of IoT devices as well as new technologies and scientific publications has soared in the past few years, the security solutions and improvements have not kept the pace. Publicly known security



breaches initiation vectors point to vulnerable and/or neglected IoT devices and the number of records stolen continues to grow. The amount of data handled by IoT devices is soaring at exponential rates, which means higher exposure of sensitive data and brings up the need to foster discussions among security researchers. Recent efforts have not been able to cover the entire security spectrum, which reveals research opportunities in different areas including smart object hardening and detection capabilities. Current issues and challenges should be taken as improvement opportunities that need to be achieved under a rigorous process that incorporates security objectives at early design stages and efficient and effective application of security standardized solutions at production stages. End users, as well, need to understand the main objective of the device and how to fulfill their requirements under strict control and scrutiny to manage the always present risk for interconnectivity.

### Notes on contributors

**Diego Mendez Mena** is a third-year Ph.D. student at Purdue University at the Center for Education and Research in Information Assurance and Security multidisciplinary program. Diego serves as well as a senior IT security analyst at Zimmer Biomet in Warsaw, Indiana. Diego obtained his Master of Science degree in Computer and Information technology at Purdue and his Bachelors' degree in Electrical Engineering at the Army's Polytechnic School in Sangolqui, Ecuador. His research interests include information security, the Internet of Things and foster STEM enthusiasm and technology innovation.

**Ioannis Papapanagiotou** is currently a senior distributed systems engineer at Netflix, a research assistant professor at the University of New Mexico, and a graduate faculty at Purdue University. He received a dual major Ph.D. degree in Computer Engineering and Operations Research from North Carolina State University and a Dipl. Ing. from the University of Patras, Greece. Ioannis has served in the faculty ranks of Purdue University (tenure-track), where he was awarded the NetApp faculty fellowship and established the Nvidia CUDA Research Center. Ioannis has also received the IBM Ph.D. Fellowship, Academy of Athens Ph.D. Fellowship, and best paper awards in IEEE GLOBECOM 2007 and IEEE CAMAD 2010. Ioannis has authored approximately 40 research articles and 10 patent disclosures. Ioannis is a member of ACM and senior member of IEEE. He focuses on distributed systems, cloud computing, Internet of things, and network systems.

**Baijian Yang** is currently an Associate Professor at the Department of Computer and Information Technology, Purdue University. He received his Ph.D. in Computer Science from Michigan State University, and his MS and BS in Automation (EECS) from Tsinghua University. He is a steering member of IEEE Cybersecurity Initiative. He holds several industry certifications, such as CISSP, MCSE, and Six Sigma Black Belt. His research interests include cyber security, data-driven security analytics, and distributed computing. In addition to academic papers, he has also published two books on Windows Phone Programming.

### ORCID

Diego Mendez Mena  <http://orcid.org/0000-0002-3813-5707>

Ioannis Papapanagiotou  <http://orcid.org/0000-0003-0907-2580>

Baijian Yang  <http://orcid.org/0000-0003-4440-3701>

### References

- Aberer, K., Hauswirth, M., & Salehi, A. (2006). A middleware for fast and flexible sensor network deployment. In *Proceedings of the 32nd international conference on very large data bases* (pp. 1199–1202).
- Acharya, R., & Asha, K. (2008). Data integrity and intrusion detection in wireless sensor networks. In *Networks, 2008. icon 2008. 16th IEEE international conference on* (pp. 1–5).
- Adolphs, P., Bedenbender, H., Dirzus, D., Ehlich, M., Eppe, U., & Hankel, M., . . . others (2015). Reference Architecture Model Industrie 4.0 (RAMI 4.0). *ZVEI and VDI, Status Report*.
- Alam, S., Chowdhury, M. M., & Noll, J. (2011). Interoperability of security-enabled internet of things. *Wireless Personal Communications*, 61(3), 567–586. doi:10.1007/s11277-011-0384-6
- Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *Communications Surveys & Tutorials, IEEE*, 17(4), 2347–2376. doi:10.1109/COMST.2015.2444095
- Alliance, Z.-W. (n.d.). *Z-wave alliance announces new security requirements for all z-wave certified IoT devices*. Retrieved May, 06 2017, from <http://z-wavealliance.org/z-wave-alliance-announces-new-security-requirements-z-wave-certified-iot-devices/>
- Atamli, A. W., & Martin, A. (2014). Threat-based security analysis for the internet of things. In *Secure internet of things (SIOT), international workshop on* (pp. 35–43).
- Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, 54(15), 2787–2805. Retrieved from <http://www.sciencedirect.com/science/article/pii/S1389128610001568> doi:10.1016/j.comnet.2010.05.010



- Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011). Proposed embedded security framework for internet of things (IoT). In *Wireless communication, vehicular technology, information theory and aerospace & electronic systems technology (wireless vitae), 2011 2nd international conference on* (pp. 1–5).
- Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, 58(1), 49–69.
- Bayram, I. S., Michailidis, G., Papapanagiotou, I., & Devetsikiotis, M. (2013). Decentralized control of electric vehicles in a network of fast charging stations. *Globecom 2013-symposium on selected areas in communications (GC13 SAC)*.
- Bilogrevic, I., Jadhwal, M., & Hubaux, J.-P. (2010). Security issues in next generation mobile networks: Lte and femtocells. In *2nd international femtocell workshop*.
- Borgia, E. (2014). The internet of things vision: Key features, applications and open issues. *Computer Communications*, 54, 1–31. doi:10.1016/j.comcom.2014.09.008
- Borgohain, T., Kumar, U., & Sanyal, S. (2015). Survey of security and privacy issues of internet of things. *arXiv preprint arXiv:1501.02211*.
- Bouhenguel, R., Mahgoub, I., & Ilyas, M. (2008). Bluetooth security in wearable computing applications. In *2008 international symposium on high capacity optical networks and enabling technologies* (pp. 182–186).
- Boyle, D., & Newe, T. (2008). Securing wireless sensor networks: Security architectures. *Journal of Networks*, 3(1), 65–77. doi:10.4304/jnw.3.1.65-77
- Caporuscio, M., Raverdy, P.-G., & Issarny, V. (2012). ubi-soap: A service-oriented middleware for ubiquitous networking. *IEEE Transactions on Services Computing*, 5(1), 86–98. doi:10.1109/TSC.2010.60
- Carriots. (n.d.). *Carriots - Internet of things platform*. Retrieved January, 16 2017, from <https://www.carriots.com/>
- Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*, 4, 2292–2303. doi:10.1109/ACCESS.2016.2566339
- Christin, D., Reinhardt, A., Mogre, P. S., & Steinmetz, R. (2009). Wireless sensor networks and the internet of things: Selected challenges. *Proceedings of the 8th GI/ITG KuVS Fachgespräch Drahtlose Sensornetze*, 31–34.
- Coetzee, L., & Eksteen, J. (2011). The internet of things-promise for the future? An introduction. In *Ist-africa conference proceedings, 2011* (pp. 1–9).
- Consortium, I. I., et al. (2015). Industrial internet reference architecture. *Industrial Internet Consortium, tech. rep.*, June.
- Corredor, I., Mart'inez, J. F., Familiar, M. S., & L'Opez, L. (2012). Knowledge-aware and service oriented middleware for deploying pervasive services. *Journal of Network and Computer Applications*, 35(2), 562–576. doi:10.1016/j.jnca.2011.05.009
- Costa, N., Pereira, A., & Serodio, C. (2007). Virtual machines applied to WSN's: The state-of-the-art and classification. In *2007 second international conference on systems and networks communications (ICSNC 2007)* (pp. 50).
- Curino, C., Giani, M., Giorgetta, M., Giusti, A., Murphy, A. L., & Picco, G. P. (2005). Mobile data collection in sensor networks: The tinytime middleware. *Pervasive and Mobile Computing*, 1(4), 446–469. doi:10.1016/j.pmcj.2005.08.003
- Curran, K., Millar, A., & Mc Garvey, C. (2012). Near field communication. *International Journal of Electrical and Computer Engineering*, 2(3), 371.
- Djenouri, D., Khelladi, L., & Badache, N. (2005). A survey of security issues in mobile ad hoc networks. *IEEE Communications Surveys*, 7(4), 2–28. doi:10.1109/COMST.2005.1593277
- Echelon. (n.d.). *Echelon - home*. Retrieved January, 16 2017, from <http://www.echelon.com/>
- Eisenhauer, M., Rosengren, P., & Antolin, P. (2010). Hydra: A development platform for integrating wireless devices and sensors into ambient intelligence systems. In *The Internet of Things* (pp. 367–373). Springer, New York, NY.
- Engineering Task Force. (2011). Extensible Messaging and Presence Protocol (XMPP): Core (RFC 6120). Retrieved from <https://tools.ietf.org/html/rfc6120.html>
- Eun, H., Lee, H., & Oh, H. (2013, February). Conditional privacy preserving security protocol for NFC applications. *Consumer Electronics, IEEE Transactions On*, 59(1), 153–160. doi:10.1109/TCE.2013.6490254
- Fernandes, E., Jung, J., & Prakash, A. (2016, May). Security analysis of emerging smart home applications. In *Security and Privacy (SP), 2016 IEEE Symposium on* (pp. 636–654). IEEE.
- Fok, C.-L., Roman, G.-C., & Lu, C. (2012). Servilla: A flexible service provisioning middleware for heterogeneous sensor networks. *Science of Computer Programming*, 77(6), 663–684. doi:10.1016/j.scico.2010.11.006
- Fongen, A. (2012). Identity management and integrity protection in the internet of things. In *2012 third international conference on emerging security technologies* (pp. 111–114).
- Forbes. (2016). *152,000 smart devices every minute in 2025: IDC outlines the future of smart things*. Retrieved December, 06 2016, from <http://www.forbes.com/sites/michaelkanellos/2016/03/03/152000-smart-devices-every-minute-in-2025-idc-outlines-the-future-of-smart-things/#34bf983369a7>
- Garcia-Morchon, O., Kumar, S., Keoh, S., Hummen, R., & Struik, R. (2013). Security Considerations in the IP-based Internet of Things draft-garcia-core-security-06. Internet Engineering Task Force.
- Gartner. (2015). *Gartner says 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015*. Retrieved December, 06 2016, from <http://www.gartner.com/newsroom/id/3165317>
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29 (7), 1645–1660. doi:10.1016/j.future.2013.01.010
- Guinard, D., Trifa, V., Karnouskos, S., Spiess, P., & Savio, D. (2010). Interacting with the SOA-based internet of things: Discovery, query, selection, and on-demand provisioning

- of web services. *IEEE Transactions on Services Computing*, 3(3), 223–235. doi:10.1109/TSC.2010.3
- Hasan, S. S., & Qadeer, M. A. (2009). Security concerns in wimax. In *Internet, 2009. ah-ici 2009. first Asian Himalayas international conference on* (pp. 1–5).
- Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., & Wehrle, K. (2011a). Security challenges in the IP-based internet of things. *Wireless Personal Communications*, 61(3), 527–542. doi:10.1007/s11277-011-0385-5
- Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., & Wehrle, K. (2011b). Security challenges in the IP-based internet of things. *Wireless Personal Communications*, 61(3), 527–542. doi:10.1007/s11277-011-0385-5
- Henrici, D., & Mu-Ller, P. (2004). Tackling security and privacy issues in radio frequency identification devices. In *International conference on pervasive computing* (pp. 219–224).
- HEU, A. B., HEU, P. G., CEA, A. O., & Stefa, J. (2013). Internet of things architecture. Retrieved from [http://www.meet-iot.eu/deliverables-IOTA/D1\\_4.pdf](http://www.meet-iot.eu/deliverables-IOTA/D1_4.pdf)
- Hong, S., Kim, D., Ha, M., Bae, S., Park, S. J., Jung, W., & Kim, J.-E. (2010). Snail: An IP-based wireless sensor network approach to the internet of things. *Wireless Communications, IEEE*, 17(6), 34–42. doi:10.1109/MWC.2010.5675776
- Huang, C.-T., & Chang, J. M. (2008). Responding to security issues in wimax networks. *IT Professional*, 10(5), 15–21. doi:10.1109/MITP.2008.110
- Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: Perspectives and challenges. *Wireless Networks*, 20(8), 2481–2501. doi:10.1007/s11276-014-0761-7
- Kasinathan, P., Pastrone, C., Spirito, M. A., & Vinkovits, M. (2013). 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)* (pp. 600–607).
- Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: The internet of things architecture, possible applications and key challenges. In *Frontiers of information technology (fit), 2012 10th international conference on* (pp. 257–260).
- Lima, R. D. C. A., Rosa, N. S., & Marques, I. R. L. (2008). Tsmid: Middleware for wireless sensor networks based on tuple space. In *Advanced information networking and applications- workshops, 2008. ainaw 2008. 22nd international conference on* (pp. 886–891).
- Lin, S. W., Miller, B., Durand, J., Joshi, R., Didier, P., Chigani, A., ... & King, A. (2015). Industrial internet reference architecture. Industrial Internet Consortium (IIC), Tech. Rep.
- Lioudakis, G. V., Koutsoloukas, E. A., Dellas, N., Kapellaki, S., Prezerakos, G. N., Kaklamani, D. I., & Venieris, I. S. (2007). A proxy for privacy: The discreet box. In *Eurocon, 2007. the international conference on "computer as a tool"* (pp. 966–973).
- Mayer, C. P. (2009). Security and privacy challenges in the internet of things. *Electronic Communications of the EASST*, vol. 17, 2009. Retrieved from <https://ubsrvweb09.ub.tu-berlin.de/eceasst/article/view/208>
- Medaglia, C. M., & Serbanati, A. (2010). An overview of privacy and security issues in the internet of things. In *The Internet of Things* (pp. 389–395). Springer, New York, NY.
- Mineraud, J., Mazhelis, O., Su, X., & Tarkoma, S. (2015). A gap analysis of internet-of-things platforms. *arXiv preprint arXiv:1502.01181*.
- Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7), 1497–1516. doi:10.1016/j.adhoc.2012.02.016
- Misra, S., Krishna, P. V., Agarwal, H., Saxena, A., & Obaidat, M. S. (2011). A learning automata based solution for preventing distributed denial of service in internet of things. In *Internet of things (ithings/cpscom), 2011 international conference on and 4th international conference on cyber, physical and social computing* (pp. 114–122).
- Murphy, A. L., Picco, G. P., & Roman, G.-C. (2001). Lime: A middleware for physical and logical mobility. In *Distributed computing systems, 2001. 21st international conference on*. (pp. 524–533).
- Naeem, T., & Loo, -K.-K. (2009). Common security issues
- Nagy, M., Katasonov, A., Khriyenko, O., Nikitin, S., Szydowski, M., & Terziyan, V. (2009). Challenges of middleware for the internet of things. In *Automation Control Theory and Practice*. Retrieved from <http://www.intechopen.com/books/automation-control-theory-and-practice/challenges-of-middleware-for-the-internet-of-things>
- Neisse, R., Steri, G., & Baldini, G. (2014). Enforcement of security policy rules for the internet of things. In *Wireless and mobile computing, networking and communications (wimob), 2014 IEEE 10th international conference on* (pp. 165–172).
- Ning, H., & Wang, Z. (2011). Future internet of things architecture: Like mankind neural system or social organization framework? *IEEE Communications Letters*, 15(4), 461–463. doi:10.1109/LCOMM.2011.022411.110120
- of California Berkeley, U. (n.d.). *Tinydb: A declarative database for sensor networks*. Retrieved January, 16 2017, from <http://telegraph.cs.berkeley.edu/tinydb/>
- of Science Thomson Reuters, W. (n.d.). *Web of science [v.5.21] - all databases*. Retrieved December, 04 2016, from <https://webofknowledge.com>
- Oka, D. K., Furue, T., Langenhop, L., & Nishimura, T. (2014). Survey of vehicle IoT blue-tooth devices. In *2014 IEEE 7th international conference on service-oriented computing and applications* (pp. 260–264).
- on Security, K. (2016). *Ddos on dyn impacts twitter, spotify, reddit*. Retrieved October, 21 2016, from <https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify>
- Park, S., et al. (2011). *Ipv6 over low power WPAN security analysis draft-6lowpan-security-analysis-05 (Tech. Rep.)*. IETF Internet Draft.

- Peppet, S. R. (2014). Regulating the internet of things: First steps toward managing discrimination, privacy, security and consent. *Texas L Reviews*, 93, 85.
- Pietzuch, P. R. (2004). *Hermes: A scalable event-based middleware* (Unpublished doctoral dissertation). University of Cambridge.
- Raymond, D. R., & Midkiff, S. F. (2008). Denial-of-service in wireless sensor networks: Attacks and defenses. *Pervasive Computing, IEEE*, 7(1), 74–81. doi:10.1109/MPRV.2008.6
- Razzaque, M. A., Milojevic-Jevric, M., Palade, A., & Clarke, S. (2016). Middleware for internet of things: A survey. *IEEE Internet of Things Journal*, 3(1), 70–95. doi:10.1109/JIOT.2015.2498900
- Rengaraju, P., Lung, C.-H., Qu, Y., & Srinivasan, A. (2009). Analysis on mobile WiMAX security. In *Science and technology for humanity (TIC-STH), 2009 IEEE Toronto international conference* (pp. 439–444).
- Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. *Computer*, 44(9), 51–58. doi:10.1109/MC.2011.291
- Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10), 2266–2279. doi:10.1016/j.comnet.2012.12.018
- Sadeghi, A.-R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial internet of things. In *Proceedings of the 52nd annual design automation conference* (p. 54).
- Sarma, A. C., & Giraõ, J. (2009). Identities in the future internet of things. *Wireless Personal Communications*, 49(3), 353–363. doi:10.1007/s11277-009-9697-0
- Sheng, Z., Yang, S., Yu, Y., Vasilakos, A., Mccann, J., & Leung, K. (2013). A survey on the IETF protocol suite for the internet of things: Standards, challenges, and opportunities. *Wireless Communications, IEEE*, 20(6), 91–98. doi:10.1109/MWC.2013.6704479
- Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in internet of things: The road ahead. *Computer Networks*, 76, 146–164. doi:10.1016/j.comnet.2014.11.008
- Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eysers, D. (2016). Twenty security considerations for cloud-supported Internet of Things. *IEEE Internet of Things Journal*, 3(3), 269–284.
- Singh, M., Rajan, M., Shivraj, V., & Balamuralidhar, P. (2015). Secure MQTT for internet of things (IoT). In *Communication systems and network technologies (CSNT), 2015 fifth international conference on* (pp. 746–751).
- Singla, A., Mudgerikar, A., Papapanagiotou, I., & Yavuz, A. (2015a). Fast and scalable authentication for vehicular internet of things. In *Proceedings of the 16th annual information security symposium* (pp. 22: 1–22:1). West Lafayette, IN: CERIAS - Purdue University. Retrieved from <http://dl.acm.org/citation.cfm?id=2775498.2775524>
- Singla, A., Mudgerikar, A., Papapanagiotou, I., & Yavuz, A. A. (2015b, October). HAA: Hardware-accelerated authentication for internet of things in mission critical vehicular networks. In *Military communications conference, MILCOM 2015-2015 IEEE* (p. 1298–1304).
- Stanford-Clark, A. N. A. (2014). Mqtt version 3.1. 1. OASIS Std., October.
- Stankovic, J. A. (2014). Research directions for the internet of things. *IEEE Internet of Things Journal*, 1(1), 3–9. doi:10.1109/JIOT.2014.2312291
- Status of project IEEE 802.11ah. (n.d.). Retrieved August, 09 2016, from <http://www.ieee802.org/11/Reports/tgahupdate.htm>
- Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the internet of things: A review. In *Computer science and electronics engineering (ICCSEE), 2012 international conference on* (Vol. 3, pp. 648–651).
- Tan, L., & Wang, N. (2010). Future internet: The internet of things. In *2010 3rd international conference on advanced computer theory and engineering (ICACTE)* (Vol. 5, pp. V5–376).
- Trends, D. (n.d.). Z-wave just made your smart home devices safer via a new security protocol. Retrieved May, 06 2017, from <https://www.digitaltrends.com/home/z-wave-security-protocol/>
- Tsao, T., Alexander, R., Dohler, M., Daza, V., & Lozano, A. (2011). A security framework for routing over low power and lossy networks. *raft-ietf-roll-security-framework-05 (work in progress)*.
- Uckelmann, D., Harrison, M., & Michahelles, F. (2011). *An architectural approach towards the future internet of things*. Springer.
- Uckelmann, D., Harrison, M., & Michahelles, F. (2011). An architectural approach towards the future internet of things. In *Architecting the internet of things* (pp. 1–24). Springer, Berlin, Heidelberg.
- Ullah, S., Ali, M., Hussain, A., & Kwak, K. S. (2009). Applications of UWB technology. *arXiv preprint arXiv:0911.1681*.
- University of California Berkeley (n.d.). TinyDB a declarative database for Sensor Networks. Retrieved from <http://telegraph.cs.berkeley.edu/tinydb/>
- Van Tilborg, H. C., & Jajodia, S. (Eds.). (2014). *Encyclopedia of cryptography and security*. New York, NY, USA. Springer Science & Business Media.
- Vermes, O., & Friess, P. (Eds.). (2012). *Internet of things: converging technologies for smart environments and integrated ecosystems*. Retrieved from <https://ebookcentral.proquest.com>
- Vidgren, N., Haataja, K., Patino-Andres, J. L., Ramirez-Sanchis, J. J., & Toivanen, P. (2013). Security threats in zigbee-enabled systems: Vulnerability evaluation, practical experiments, countermeasures, and lessons learned. In *System sciences (HICSS), 2013 46th Hawaii international conference on* (pp. 5132–5138).
- Weber, R. H. (2010). Internet of things – New security and privacy challenges. *Computer Law & Security Review*, 26(1), 23–30. doi:10.1016/j.clsr.2009.11.008
- Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law & Security Review*, 31(5), 618–627. doi:10.1016/j.clsr.2015.07.002

- Weis, S. A., Sarma, S. E., Rivest, R. L., & Engels, D. W. (2004). Security and privacy aspects of low-cost radio frequency identification systems. In *Security in pervasive computing* (pp. 201–212). Springer, Berlin, Heidelberg.
- Weyrich, M., & Ebert, C. (2016). Reference architectures for the internet of things. *IEEE Software*, 33(1), 112–116. doi:10.1109/MS.2016.20
- Xively. (n.d.). *Xively by logmein: IoT platform for connected devices*. Retrieved January, 16 2017, from <https://www.xively.com/>
- Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for internet of things. *Journal of Network and Computer Applications*, 42, 120–134. doi:10.1016/j.jnca.2014.01.014
- Yavuz, A. A., Mudgerikar, A., Singla, A., Papapanagiotou, I., & Bertino, E. (2017). Real-time digital signatures for time-critical networks. *IEEE Transactions on Information Forensics and Security*, PP(99), 1.
- Zafari, F., & Papapanagiotou, I. (2015). Enhancing iBeacon based micro-location with particle filtering. In *Global communications conference (globecom), 2015 IEEE* (pp. 1–7).
- Zafari, F., Papapanagiotou, I., & Christidis, K. (2015). Micro-location for internet of things equipped smart buildings. *CoRR, abs/1501.01539*. Retrieved from <http://arxiv.org/abs/1501.01539>
- Zafari, F., Papapanagiotou, I., & Christidis, K. (2016, February). Microlocation for internet-of-things-equipped smart buildings. *IEEE Internet of Things Journal*, 3(1), 96–112. doi:10.1109/JIOT.2015.2442956
- Zafari, F., Papapanagiotou, I., Devetsikiotis, M., & Hacker, T. J. (2017). An iBeacon based proximity and indoor localization system. *CoRR, abs/1703.07876*. Retrieved from <http://arxiv.org/abs/1703.07876>
- Zhao, D., & Raicu, I. (2013). HyCache: A user-level caching middleware for distributed file systems. In *Parallel and distributed processing symposium workshops & PhD forum (IPDPSW), 2013 IEEE 27th international* (pp. 1997–2006).
- Zhao, K., & Ge, L. (2013). A survey on the internet of things security. In *Computational intelligence and security (CIS), 2013 9th international conference on* (pp. 663–667).
- Zhou, L., & Chao, H.-C. (2011). Multimedia traffic security architecture for the internet of things. *Network, IEEE*, 25(3), 35–40. doi:10.1109/MNET.2011.5772059
- ZigBee Alliance (2006). Zigbee security specification overview. Retrieved from [http://read.pudn.com/downloads55/ebook/189874/ZigBee\\_Security\\_Layer\\_Technical\\_Overview.pdf](http://read.pudn.com/downloads55/ebook/189874/ZigBee_Security_Layer_Technical_Overview.pdf)
- Zuehlke, D. (2010). Smart factory towards a factory-of-things. *Annual Reviews in Control*, 34(1), 129–138. doi:10.1016/j.arcontrol.2010.02.008