

Internet of Things: Survey on Security and Privacy

Diego Mendez¹, Ioannis Papapanagiotou², Baijian Yang³
Purdue University

Abstract—The Internet of Things (IoT) is intended for ubiquitous connectivity among different entities or “things”. While its purpose is to provide effective and efficient solutions, security of the devices and network is a challenging issue. The number of devices connected along with the ad-hoc nature of the system further exacerbates the situation. Therefore, security and privacy has emerged as a significant challenge for the IoT. In this paper, we aim to provide a thorough survey related to the privacy and security challenges of the IoT. This document addresses these challenges from the perspective of technologies and architecture used. This work focuses also in IoT intrinsic vulnerabilities as well as the security challenges of various layers based on the security principles of data confidentiality, integrity and availability. This survey analyzes articles published for the IoT at the time and relates it to the security conjuncture of the field and its projection to the future.

Index Terms—Internet of Things, Security, Privacy, Embedded Devices, Confidentiality, Integrity, Availability

I. INTRODUCTION

THE essence of the Internet of Things (IoT) is the concept of every device blending with the existence of human beings. It is the state wherein there is no distinguishable difference between the operation of devices surrounding us and our actions. This means that devices become part of our experience. There is a seamless integration between us and the “things” around us. The various devices communicate intelligently with one another to execute daily operations. There is minimal human intervention for the operation of devices. Every device is connected to every other device, communication with one another, transferring data, retrieving data and intelligently responding, triggering actions. The successful implementation of the IoT involves consideration of a huge number of aspects. These involve the technology used for communication, various communication protocols which form the backbone of the IoT, standards to be used for communication, hardware and embedded devices used to build the hardware, the software, operating system that is compatible with hardware and the protocols being used. By the end of 2020 it is said that there would be around 20 billion connected devices [1]. The data exchanged over the network will be greater than 40 Zettabytes for the same period [2]. This brings up an important discussion regarding all the data generated, stored or transmitted by IoT devices, its security and how this

relates to the privacy of the users. 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 systems are built with security as one of the central aspects of the IoT. This paper discusses the security issues at different levels of the IoT system. It presents an exhaustive survey of security and privacy issues existing in IoT systems, its enabling technologies and protocols. This paper elaborates on the current status of the field, providing the big picture based on IoT Architecture, analyzes the security challenges and vulnerabilities of the different underlying technologies and protocols, discusses the IoT security concerns under the security triad perspective and explores the current privacy issues of IoT systems under different points of view. Finally, summarizes the content to give a clear perception of the ongoing security challenges of the IoT and overlays some solutions.

II. STRUCTURE OF IOT SYSTEMS

The IoT heterogeneous essence, dynamics, intelligence, mobility and undefined perimeters makes it a high-demand technology domain but also makes the IoT vulnerable and risky under security terms. The different platforms where the IoT is available makes 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 for ubiquitous computing, whose goal is to connect everyday life objects to the network using technological platforms, is made up of three components [3]:

- (a) Hardware
- (b) Middleware
- (c) Presentation

Also, the same pattern can be observed when determining the paradigms of the IoT, according to [4] and [3] three factors can be attributed to the IoT environment, those are:

- (a) Internet-oriented
- (b) Things-oriented
- (c) Semantic-oriented

Therefore, the same concept can be applied to the IoT structure. The IoT architecture, according to [5] is composed of three layers:

- (a) The perception layer
- (b) The network layer
- (c) The application layer

The perception layer gathers environmental data, the network layer, which is composed of wired and wireless systems,

1. Diego Mendez is with Purdue University, West Lafayette, IN, 47907.

E-mail: dmendezm@purdue.edu

2. I. Papapanagiotou is with Netflix Inc., Los Gatos, CA 95032 and Purdue University, West Lafayette, IN, 47907.

E-mail: ipapapa@ncsu.edu

3. Baijian Yang is with Purdue University, West Lafayette, IN, 47907.

E-mail: byang@purdue.edu

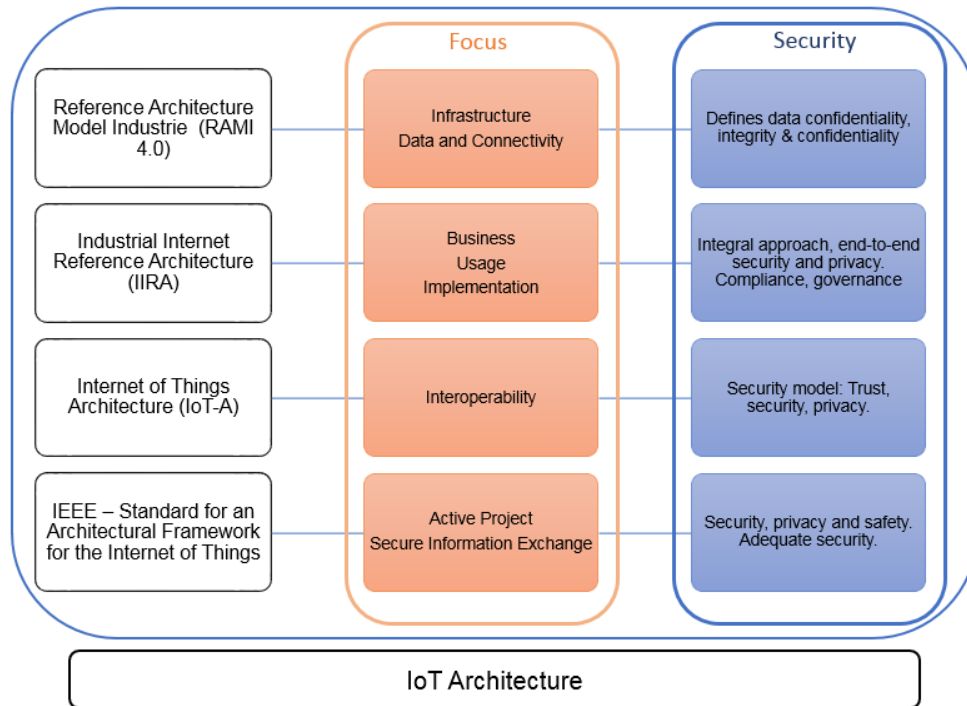


Fig. 1. Current IoT Architecture Frameworks/Standards

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 [6]. Figure 1 summarizes current IoT architecture frameworks/standards and highlights their security objectives.

However, there is no unified view of the IoT framework. Some engineering bodies, including the IEEE and ETSI, have issued technology-specific standards including security guidelines [5]. These standardization efforts have also brought up other initiatives for unified architecture and modeling, for instance the Reference Architecture Model Industrie 4.0 (RAMI 4.0) [7], the Industrial Internet Reference Architecture (IIRA) [8] and the Internet of Things - Architecture (IoT-A) [9]. 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 unification attempts are needed for simplification, always taking security communications as the main actor and enabler of IoT initiatives [6]. Besides the industrial domain, the scientific community has been a main contributor of the standardization of IoT protocols and technology as well [4]. The author of [10] advocates 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 [11] back a reliable architecture that address security and service requests. From a different perspective, the authors of [12] promote the importance of robust and reliable standards to conduct shielded

IoT architectures, currently required with insistence from the security community.

III. VULNERABLE LANDSCAPE

Security issues of IoT devices occur in different instances which include technological, ethical and privacy concerns. 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 (DNS) infrastructure - by a botnet army of IoT infected devices, has turned on the alarms on the consequences that faulty IoT protections and poor standards can motivate [13] which accentuates the need for additional research on the IoT security domain. Nevertheless, the number of publications addressing security issues and concerns for the expanding Internet of Things has not foster 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 five years [14]. Figure 3 shows a basic comparison of the number of publications for both subjects. In despite of the issues presented above, there is some important discussion taking place between experts about what the baseline for secure IoT systems. For instance, according to [15], 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 [16], has also determined similar security requirements for the Internet of Things, which include: (a) attack resiliency,

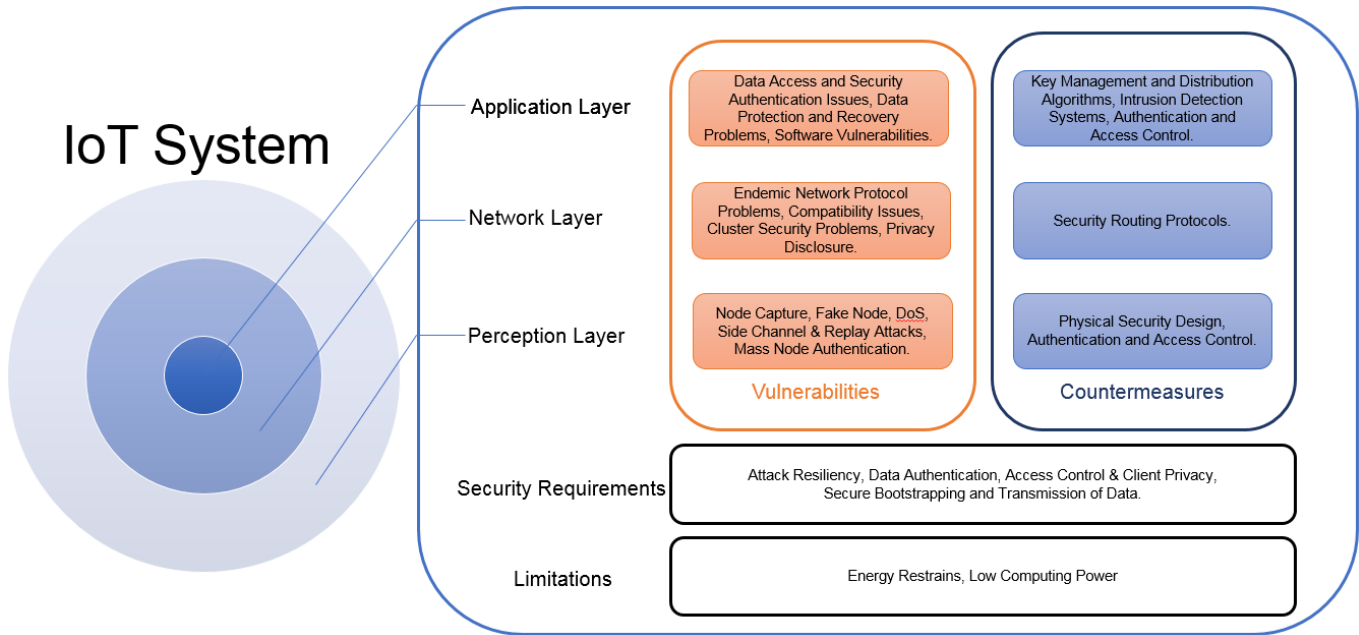


Fig. 2. Internet of Things Security Landscape.

(b) data authentication, (c) access control, and finally demand (d) client Privacy. Also, [5] proposes 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 finally, (f) physical security design.

For [17], [18], 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 Internet of Things 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 [19]. IoT devices are also exposed to physical tampering, war driving, malicious software and side-channel attacks [19].

Security problems of the Internet of Things need to be understood in order to find an appropriate solution (Figure 2). The vulnerable landscape can be scrutinized from an architectural perspective; the perception, the network and the application layer present security problems of their own that need 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, [20] states that 55% of Samsung-owned SmartThings development platform applications are overprivileged and therefore present important security risks.

IV. ENABLING TECHNOLOGIES AND PROTOCOLS

The Internet of Things (IoT) may be powered by different technologies with different 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 [21], and specifically related to the external adversary entity. The authors of [21, p. 38] refer to the 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".

A. Perception Layer

1) *Wireless Sensor Networks*: The authors in [22, p.65] defined Wireless Sensor Networks (WSN) "as a group of independent nodes communicating wirelessly offer limited frequency and bandwidth", which in order to perform successfully depend on a massive 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 [3] the WSN network module include 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 is shared

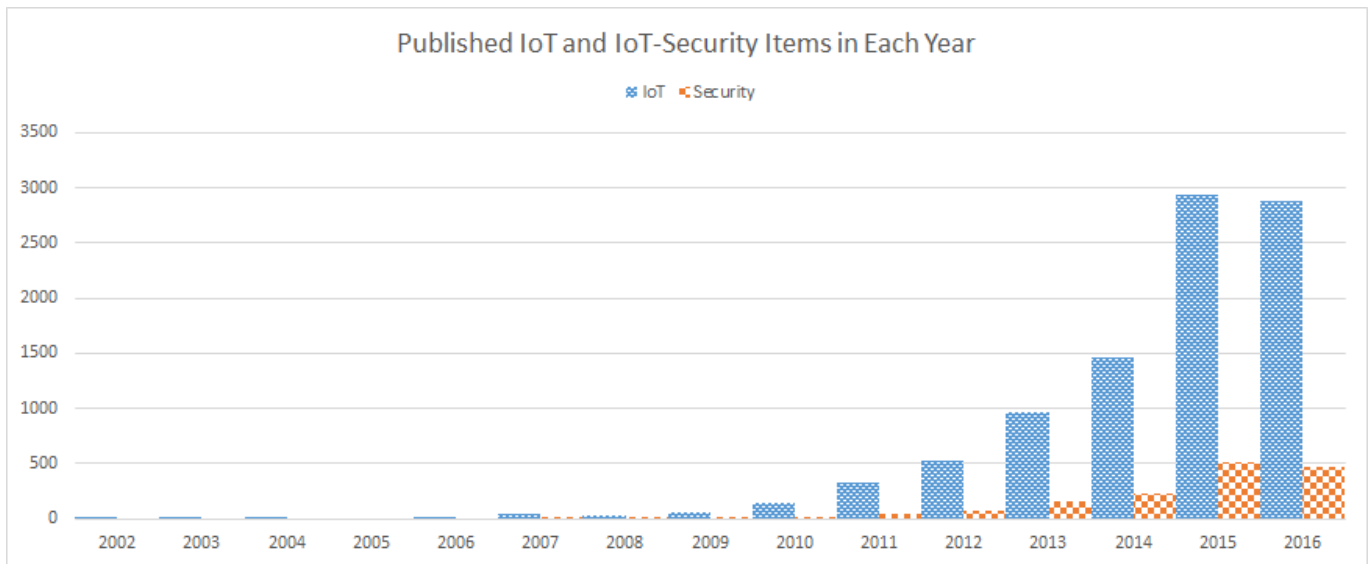


Fig. 3. Number of publications for Internet-of-Things and Internet-of-Things Security related articles. As of December 2016 [14].

between them or by a centralized system for analytic purposes [3].

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 [23]. WSNs, as well as other network applications, require measures against common attacks and rises which include Denial of Service (DoS), traffic analysis, node replication (Sybil attack), general confidentiality concerns, black hole routing attacks and physical damage / unauthorized manipulation [22]. [22, p.66] also mention 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. Moreover, some security requirements are set in order to consider WSN nodes as secure, which include:

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

WSNs vulnerabilities, according to [23], 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 [23].

Authors of [24] affirm 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 mention 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 in some aspects, by the use of authentication methods through Public Key Infrastructure (PKI), to prevent rogue node data injection, and authorization technologies to mitigate DoS risks [25].

According to [22], node authentication can solve most of the problems that may be caused by unauthorized uses, some of the authentication methods disused take into account SPINS, composed of Secure Network Encryption Protocol (SNEP), micro-Tesla, TINYSEC, Localized Encryption and Authentication Protocol (LEAP/LEAP+) and Zigbee.

2) *Radio Frequency Identification*: Radio Frequency identification (RFID) implementations provide unique identification based on passive tags to the items they are attached to. The data transmitted from the scan reading is commonly "unprotected or read-only" [25, p.391], including Ultra High Frequency (UHF) and Global Gen-2 tags under default settings. RFID passive tagging, by default, permits reading by any compliant scanner with no authentication at all, increasing ears

dropping risks and relegating passive RFID solutions to non-critical settings [25]. RFID vulnerabilities can be classified as the following: (a) attacks on authenticity, i.e. unauthorized tag disabling, (b) attacks on integrity, i.e. unauthorized tag cloning, (c) attacks on confidentiality, i.e. unauthorized tag tracking and (d) attacks on availability, i.e. replay attacks [23]. Also, Corporate espionage risks, location as well as personal privacy concerns may be affected by the use of unprotected tags [26]. Usually, many RFID implementations are exposed to physical and traffic analysis attacks [27], based on their autonomous properties, RFID devices respond automatically to readers' requests makes them inherently vulnerable [28]. Back in 2004 and 2005, proof-of-concept attacks have been published against RFID financial transactions disclosures as well as cryptographic keys brute-forcing for widely deployed RFID tags [29]. Even Advanced Encrypted Scheme (AES) RFID solutions may present security vulnerabilities a those devices, based on the passive power capabilities, are susceptible to "fault induction, timing attacks or power analysis attacks" [26, p.203].

Zhao & Ge [5] provide security measures to secure RFID communications, which include: (a) access control, that protect RFID tags against reading at will, (b) data encryption, which include non-linear key algorithms, (c) IPSec protocol utilization, (d) cryptography technology scheme, to protect against side-channel attacks, i.e. Differential Power Analysis (DPA) attacks by eliminating "data dependencies of the energy consumption" and also by obscuring the encryption process values based on randomization [5, p.666], however, DPA attacks are not protocol-dependent as it may be used against other communication procedures. [28] has also presented a new lightweight implementation using the recent SHA-3 appointed function Keccak-f(200) and Keccak-f(400) to secure RFID applications through hashing functions. [27] proposes more simple solutions based on "tag killing", which is not satisfactory, and "Blinded Tree-Walking" to take advantage the backward channels to prevent eavesdropping attacks. Nevertheless, both approaches do not address location privacy issues. [27] also presents "Blocker Tags" solutions to provide user privacy by blocking readers' requests using the anti-collision algorithm embedded in RFID systems to differentiate between tags. Other solutions propose ciphertext re-encryption to hide communication appearance by using encryption-capable tags which usually do not offer a cost-effective solution [27]. [29] promotes the development of security standards not only for emerging RFID technologies to address security issues but also to solve other interaction issues, which can be seen as a win-win situation for not-security-focused developers. [26] also proposes a hashed based access control by using hardware-optimized functions as well as randomized access control to prevent user tracking by using hash functions and random number generators in order to control the predictability of responses from RFID tags.

3) *802.11*: The current IEEE 802.11 standard, 802.11ac or 802.11n i.e. Wi-Fi is wireless Local Area Networking technology that connects electronic devices within the range of 100m to the network. IEEE has developed 802.11ah Task Group that is focused on developing a wireless communication

standard based on 802.11 which is suitable for the specific needs of IoT systems. The main intent of the task group is to eliminate the existing capability and capacity gaps. IEEE 802.11 networks are vulnerable, as any other wireless network, to easily performed passive attacks, including eavesdropping just armed with suitable receiving antennas [30]. However, active attacks can be performed as well by exploiting protocol and hardware vulnerabilities including jamming and scrambling attacks [31]. The current 802.11ah development and design requirements also try to implement security based on the properties of IoT devices, such as constrained memory and limited power supply, in order to include them in early stages to ensure proper functioning when fully deployed [32].

4) *Long Term Evolution (LTE)/LTE-Advanced*: IoT Systems depend on gateways to reach the Internet in an efficient way, for areas where the wired gateways are not an option usually Long Term Evolution (LTE) devices are chosen to fulfill that purpose based on bandwidth, coverage and spectrum efficiency [33]. LTE Femtocells, which are used as low-range and low-power radio bases designed for small scale users or systems, provide the connection to the core cellular network. Such low-tier cells level the ground that eventually fosters the spread use of LTE and its significance [34]. According to [34], "Security and Privacy in such networks is achieved at several levels in their air architectures, such as the air interface, the operator's internal network and the inter-operator links" [34, p. 1]. As any other wireless technology, LTE networks are susceptible to passive and active attacks, although some active attacks can be controlled by the use of cryptographic tools. Passive attacks, such as traffic analysis and accurate user tracking are nearly impossible to contain [34]. Femtocells are also vulnerable to tampering as attackers may find them easier to access than any other LTE infrastructure, which can lead to undetected privacy exposure. Moreover, Femtocells are exposed to other kind of attacks, including impersonation, false reporting of location that may affect the normal operation of the device [34]. Exposure of public IP addresses of gateways, such as Femtocells, could leave the LTE core network vulnerable to internet-originated attacks, such as DoS, DDoS and impersonation attacks as well [34]. Some solutions proposed to address identity and location tracking is by the implementation of adaptive schemes that change the identifiable information based on the context of the communication or by demand of the user [34].

5) *WiMax*: While the technology has lost its popularity, it can still be used to connect different IoT devices particularly in metropolitan areas. The higher data rate accompanied by longer range can certainly facilitate different entities particularly in remote areas. IEEE 802.16 security specifications reside primarily within the MAC layer, such specifications reside on what is called a 'security' or 'privacy' sublayer [35], therefore, the physical layer remains mainly unprotected [36]. Some of the security concerns associated with WiMAX are jamming at physical layer that can result in denial of service [36] or network mapping by eavesdropping [37]. Nevertheless, the MAC layer also presents security issues such as Man-in-the-middle attacks, caused by rogue Base Station (BS) that pretends to be a legitimate BS, replay attacks and Denial

or downgrade of service due to flawed authentication and resource limitation, which includes cryptographic computer efficiency constraints [38]. [39] proposes the incorporation of additional schemes for authentication and key distribution that nevertheless still have efficiency issues to be improved before becoming introducing into real applications.

6) *Near Field Communication*: Near Field Communication (NFC) has a short range of 20 centimeters, however it can be used for wide range of services in IoT systems such as payments, authentication, data exchange, etc. From the security perspective, NFC is also prone to a number of threats including Denial of Service (DOS), and information leakage [40]. The major security issue with NFC is that for some cases it is not encrypted, i.e. to maintain backward compatibility with RFID. Therefore, it results in security vulnerability as the wireless signal generated by the devices can be picked up by antennas [41]. NFC is also prone to eavesdropping in active mode. It is possible as well to implement an NFC skimmer device that could listen to the NFC communication between any two near-by devices. The data could be stored and collected later just like many ATM devices. It can also be manipulated by interfering with the data channel making the data corrupted and useless when it arrives at the destination. Similarly, the NFC tag can be modified by potential attackers who can replace the original tag with a fraudulent one with the intent to steal valuable user information. [42] proposes a security model for NFC that provides conditional privacy protection. This method is based on the use of random public keys like pseudonyms. These keys are generated based on the long-term key issued by the Trusted Service Manager. This suggested method can protect user's identity and provide conditional privacy.

7) *Bluetooth*: Bluetooth is certainly a viable technology for IoT systems. It has already been adopted for indoor proximity systems in form of iBeacons [43]. Due to its range and data throughput, it can also be used in different sensor networks for various tasks such as earthquake monitoring. The Bluetooth protocol it is designed to provide security in 3 ways: (1) use of pseudo-random frequency hopping, (2) Restricted authentication and (3) Encryption [44]. Even though the generic access protocol of Bluetooth make possible three security modes: (1) Non-Secure, (2) Service-levels security and (3) Link-level security, there are still security concerns that need to be addressed. [45] lists some vulnerabilities that persists even after the security features have been introduced, which includes optional or weak encryption, non-secure default settings, weak PIN use, insecure unit keys, flawed integrity protections and predictable number generation. Bluetooth is also prone to a number of threats including eavesdropping, Man-In-The-Middle attacks, data corruption, and denial of service. Attackers have also paid attention to vehicle IoT Bluetooth pairing applications and devices making them a valuable target that need to be secured [46], [47]. Nevertheless, [44] proposes some simple solutions that address some of the security flaws, which include: User understanding of the technology, centralized Bluetooth pairing policy implementation, use of non-discoverable mode or on-demand access/pairing and mandatory encryption use. Bluetooth has

also been used for microlocation purposes through beacons enabled by Bluetooth Low Energy (BLE) technology [48], [49] or proximity applications [50]. BLE communication is conformed by the interchange of small data packets which are broadcast, one-way only, within an specific time [51]. As expected, the data processed by beacons and BLE systems may contain private user data that need to be protected from intruders and from indiscriminate use [51]. BLE uses AES-128 CCM for encryption and authentication purposes [17].

8) *ZigBee*: Based on the IEEE standard 802.15.4, the ZigBee protocol defines the network (NWK) layer as the one that runs on top of the physical (PHY) and MAC layers. It also comprehends descriptions, algorithms and protocols for the application support (APS), which outlines the device objects (ZDO), the device profile (ZDP) and the security services. The present security architecture consists of the ZigBee coordinator which performs network joining and key distribution duties, here the Thrust Center concept was introduced, which plays three roles:

- Trust manager
- Network manager
- Configuration manager

The trust manager authenticates the devices requesting to join the network, the network manager maintains and distributes network keys and the configuration manager provides end-to-end security between devices [52]. ZigBee also offers two operation modes, residential and commercial, where the first one offers no security and the second one provides a centralized key management scheme and maintains freshness counters with other devices in the network. This gives centralized control and the ability to update keys. The three different types of keys are the Master key, Link Key and Network Key. The Master Key is part of the factory-setting. They are from the Trust Center and are the basis for long-term security between devices. The network Keys are shared by all the devices on the network and are the basis for security over the entire network. The Link Key is shared by two devices and is the basis for the security between the devices. The use of the different keys ensures the freshness and integrity of the data. ZigBee uses AES-128 with CCM (CCM = CBC-MAC = Counter with Cipher Block Chaining Message Authentication Code) mode for data encryption and authentication. However, some trade-offs must be made between security, power consumption and latency (Boyle & Newe, 2008). According to [53], Zigbee-enabled systems are susceptible to threats such as traffic sniffing (eavesdropping), packet decoding, and data manipulation/injection, which can be exploited by an attacker who uses a special hardware and software developed especially for attacking purposes. Other vulnerabilities that a ZigBee enabled network is susceptible to are physical device damage and key sniffing attacks.

A similar proprietary approach is brought by Z-Wave, backed up initially by Intel and Cisco [54]. Z-Wave has an architectural similarity with Zigbee with a few differences that makes Z-Wave a more approachable technology for home-automation systems. According to [55], Z-Wave uses AES encryption for secure communication, however, it presents two

main vulnerabilities. The first one deal with the hard-coded encryption key embedded in the Z-Wave chip, an attacker may intercept the key exchange messages and use the hard-coded key to unveil the content. The second one deals with the lack of validation of the key exchange protocol handler which can allow an attacker to inject packets to the key exchange process and take control of the device. A security feature, noted by [54], includes the procedure to add new devices to the network that forces the new device to be within one meter for set-up, which limits the attack ratio. Additionally, as a response to recent hijacking of IoT devices the Z-Wave Alliance has come up with the security framework S2 [56]. The alliance, fortunately, has made the implementation of the new framework mandatory and, therefore, improved the embedded security by strengthening the pairing process for new devices [57].

9) *Ultra-Wideband*: The low power and higher precision make it suitable for the IoT and smart architecture applications as well including the provision of micro-location services for tenants of IoT-equipped smart buildings. From security perspective, literature shows the UWB is comparatively secure and is suitable for IoT applications due to its processing power, range, data rate and security. Indeed, it is already considered as a viable technology for Wireless Body Area Networks (WBANs) and can be used for a number of different services including smart health care system. UWB signals secure and highly reliable particularly in health applications [58].

10) *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, Zhengguo, et al. [59] the key features of IPv6 which makes it suitable 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, S., et al. [60] 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, neighbor discovery attacks. (d) An attack against the transport layer is performed by half open, half closed 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 (SeND) extended to support Elliptic Curve Cryptography (ECC) encryption algorithm which uses smaller-packet sizes compared to RSA and secure key management algorithms engineered to suit the specific characteristics of 6LoWPAN.

B. Middleware

The challenges presented by the IoT can present issues between each one of the architectural components of embedded systems, therefore, middleware has been developed in order to interconnect and integrate all the elements that make the IoT possible. Middleware in the IoT is used as well to interact with “cloud technologies, centralized overlays, or peer to peer systems”. Evidently, the attack surface increasing 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 [61]. The authors of [61, p.76] proposes seven categories for discussion based on design principles:

1) *Event-based*: According to [61] all the participants in the middleware connect through events, the events consist of a set of parametric values that describe specific changes of state. Some event-based middleware applications present security features and some others do not consider security requirements at all. For instance, HERMES [62] utilizes a security module that controls the perimeter based on access control, it also provides confidentiality between brokers through X.509 certificates and OASIS role memberships. Other applications such as EMMA, GREEN, RUNES, Steam, MiSense, PSWare and TinyDDS do not show specific security features [61].

2) *Service-oriented*: [61] describes service-oriented middleware to the design approach that constructs applications as services, similar to service-oriented computer (SOC) that is based on service-oriented architecture (SOA) for common Information Technology (IT) systems. Service-oriented applications include security attributes as well as vulnerabilities. HYDRA [63] employs a security manager as part of its management components design, each one of the components take care of application and device elements, which have an additional security layer. It applies a distributed security as well as trust elements for securing inter-device connections, it also uses virtualization to provide security and privacy,

which according to [61] may introduce vulnerabilities for side-channel attacks. SOCRADES [64], introduces role-based access control for device communication with the application, however, its security features is limited to authentication only. UbiSOAP [65] uses some functions from its resource layer to authenticate components for security and privacy. Servilla [66] presents privacy concerns due to the access level it provides to individual sensors [61]. KASOM [67], uses a security manager which is part of one of the major subsystems, however, it offers security by authentication only [61]. Xively [68] provides support for end-to-end security for the entire system which provides integrity, however, it does not provide security for its storage components [69] same for CarrIoTs [70]. Echelon [71], according to [61], does not include any security mechanism. Other applications, such as SenseWrap, MUSIC, TinySOA, SensorsMW, SENSEI, KASOM, CHOReOS, MOSDEN and WhereX do not show specific security components for analysis [61].

3) *Virtual Machine (VM) based:* [61] classifies middleware as VM-based the applications that use virtual infrastructure for the purpose of safe execution. The applications are built from specialized modules, which can be spread through the network, where each node runs a VM that interact with the modules. The middleware application Maté [72] has a system component dedicated to security, its purpose is to block the propagation of harmful programs through the network. Other applications, such as VM, Melete, MagnetOS, Squawk, Sensorware, DVM, DAViM, SwissQM and TinyReef do not show any specific security features for analysis according to [61].

4) *Agent-based:* Agent-based middleware is composed of modular programs that “facilitate injections and distribution through the network using mobile agents”. Agent-based middleware deserve as well a security-focused analysis for features and vulnerabilities. The application Ubiware [73] adds policies to support the security requirements of the middleware. Other solutions, such as Impala, Smart Messages, ActorNet, Agilla, UbiROAD, AFME, MAPS, MASPOT, and TinyMAPS, do not present security or privacy demands [61].

5) *Tuple-spaces:* Tuple-space middleware each component contains a data repository or tuple space that can be accessed simultaneously [61]. Applications such as LIME [74], TinyLIME [75] and TS-Mid [76] do not support any security or privacy mechanism [61].

6) *Database-oriented:* The sensor network acts as a “virtual relational database system” that can be queried by SQL-alike language. Under the security domain, current database-oriented middleware solutions, such as GSN [77] and HyCache [78] do not deal with security or privacy requirements. TinyDB [79] does not show any security feature for analysis according to [61].

7) *Application-specific:* Application-specific middleware specializes on managing resources for specific requirements demanded by the application or by the domain it works on [61]. Given the nature of application-specific middleware the solutions developed under these architecture cannot satisfy general IoT requirements taken into account in other appli-

cations in terms of heterogeneity, therefore, security demands cannot be satisfied integrally [61].

C. Application Layer

1) *Message Queue Telemetry Transport (MQTT):* The characteristics of the various devices used in Internet of Things is such that they lack the capability to handle high-level protocols like HTTP. Researchers are more inclined on developing light-weight protocols that suit the specific characteristics of IoT devices. The Message Queue Telemetry Transport (MQTT) proposed by Andy Stanford-Clark, and Arlen Nipper [80] 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. Identity specifies the client that is being authorized. Authentication provides identity of the client and authorization is the management of rights given to the client. 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 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 server and what topics a client can publish or subscribe to. According to Neisse [81] the security controls provided by MQTT are not sufficient for the IoT network. IoT networks requires “data anonymization, obfuscation or dynamic context-based policies that should be dynamically evaluated for each message forwarded by the broker” [81, p. 1]. Neisse [81] implements 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. [82] proposes a new security solution for MQTT (Secure MQTT or 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 (ABE) over elliptic curves.

2) *Extensible Messaging and Presence Protocol (XMPP):* The Extensible Messaging and Presence Protocol 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 [83]. XMPP architecture is defined by a distributed network of clients and servers. The recommended ordering of layers in XMPP described in [83], 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 is processed in cleartext on the sender's and the receiver's servers. It is also unprotected when it is sent from sender's to receiver's server, or sent from receiver's server to receiver's client. Systems using XMPP as the enabling 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.

3) *Blockchain*: Blockchain [84] 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 trustless 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 trustless, simple techniques, such as whitelisting, 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.

V. 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 becomes 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 [94]. 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 [95], [96], [97], [98].

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, Denial of Service attacks, brute-force attacks, traffic injections, etc [99]. According to [3, p. 14], 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" is the application of cryptographic features. Encryption schemes protect confidentiality as message authentication codes assures integrity as well as authenticity. Former WSN implementations, according to [100], 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 [101], in order to enable massive adoption of Internet of Things devices; security, including confidentiality, integrity, availability, and privacy issues must be addressed in order to make them trustworthy to the public. [101] suggests 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 [25].

IEEE standard 802.15.4, which provides guidelines to protect physical and medium access control layers, may be used as a instrument to add security features that sum up confidentiality, integrity and availability properties to the system [25]. The Internet Draft ID-Tsao [102] signals a high-level presentation of the existing threats and security countermeasures in terms of the security triad. [103] indicates a potential limitation of the framework based on the non-differentiation arguments and layer 3-only analysis.

A. Confidentiality

[85, p.1505] defines data confidentiality as a "fundamental issue" for IoT solutions, "particularly relevant in the business context". [85] also indicates 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 [85] also mention proper identity management as a key factor to assure data confidentiality. Some IoT devices need to handle data need 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

TABLE I
COMPARISON BETWEEN MOST CITED PUBLICATIONS FOR IOT SECURITY [14]

	<i>Gubbi et al. (2013) [3]</i>	<i>Miorandi et al. (2012) [85]</i>	<i>Bandyopadhyay et al. (2010) [86]</i>	<i>Roman et al. (2011) [87]</i>	<i>Zhou et al. (2011) [88]</i>	<i>Hong et al. (2010) [89]</i>	<i>Zuehlke (2010) [90]</i>	<i>Sarma et al. (2009) [91]</i>	<i>Roman et al. (2011) [92]</i>	<i>Yan et al. (2014) [93]</i>
Enabling Technologies	<i>WSN</i>	✓		✓		✓			✓	✓
	<i>RFID</i>	✓			✓	✓	✓		✓	✓
	<i>Ultra-Wide Band</i>									
Low-Level Protocols	<i>802.11</i>									
	<i>LTE/LTE advanced</i>									
	<i>NFC</i>			✓						
	<i>Bluetooth</i>									
	<i>6LoWPAN</i>						✓		✓	✓
	<i>ZigBee</i>						✓			
	<i>MQTT</i>									
High-Level Protocols	<i>XMPP</i>									
	<i>Blockchain</i>									
	<i>Confidentiality</i>	✓	✓	✓	✓	✓	✓		✓	✓
Security Triad	<i>Integrity</i>	✓	✓		✓	✓	✓		✓	✓
	<i>Availability</i>	✓	✓	✓	✓		✓		✓	✓
	<i>Authorization</i>		✓		✓	✓		✓	✓	✓
AAA	<i>Authentication</i>	✓	✓	✓	✓	✓	✓	✓	✓	✓
	<i>Accounting</i>							✓		
	<i>Privacy</i>	✓	✓	✓	✓		✓	✓	✓	✓

system as stated by [104]. 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 [103]. [105] emphasizes on the importance of confidentiality research and the inherent challenges attached to it. [105] also indicates the importance of authenticity and the integrity of data groundwork as well. The confidentiality needed for a sensor data, according to [105], 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. [94] states that the major confidentiality sensitivity, in the IoT context, 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. [94] believes that there is adequate research work available for communication, storage, localization/tracking, and identification subjects, although, [94] recognizes the complexity of employing current mechanisms for securing the IoT. According to [106, 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, [107] indicates 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 [108]. [109] proposes 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 [103]. In order to protect data and communication confidentiality, some cloud-based solutions establish secure channels based on cryptographic features relying on Public Key Infrastructure (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 [108].

According to [86], privacy of humans and business confidentiality are two major issues to be addressed for the Internet of Things. Standard encryption schemes may solve the problem, however, energy and processing resources need to be efficiently applied, including key distribution mechanisms, to be considered as a valid IoT solution. Confidentiality and Privacy are usually tied together, according to [10, p. 622], “Privacy as confidentiality represents solutions for anonymizing the collected data (including communications) and minimizing the collection of data”. [10] also suggests 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. [10] also indicates 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 [108]. [110] states 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 [85], data confidentiality, privacy and trust are key factors that can leverage the widespread adoption of IoT technologies and applications.

B. 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 [111]. Another critical factor that influences data integrity is the robustness and fault tolerance capabilities of the IoT System [85]. 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 [4].

Integrity for the Internet of Things 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 Multi Level Security (MLS), help 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 [112]. Hardware

solutions have also been proposed for integrity purposes, a challenge-based solution is mentioned in [112] by the use of symmetric or asymmetric keys known as Trusted Platform Module (TPM).

Process integrity is also required by IoT devices, process integrity 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 [94]. 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 [111]. 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 [113]. 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 “swarn attestation” that allows software integrity verification collectively from multiple devices or “provers” [111].

Authentication schemes used in the IoT not only tries to assure the identity of an object but also attempts to assure its integrity. Authentication, through Identity Management (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 a IoT infrastructure after facing scalability, capability and management issues [112]. 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 [85].

C. Availability

Usual information networks, according to [105, p. 648], need to guarantee “identification, confidentiality, integrity and undeniability”, nevertheless, IoT networks that can potentially be utilized in “crucial areas of national economy”, which need as well to pay special attention to availability and dependability. According to [114, p. 601], for information networks, device availability is the “most important factor”. IoT availability requirements, as specified by [115], 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, [116] proposes that in order for IoT devices to reach their potential they will need to address requirements, such as availability, which, by the way, it is listed as a one of the key challenges to be addressed for the IoT. [116, p. 2362] also indicates 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 [59], some constrained devices may face similar effects as a Denial-of-Service (DoS) attack from huge amounts of legitimate clients’ requests that may hinder the services provided. Still, current Internet Engineering Task Force (IETF) standardized communication protocols, such as Constrained Application Protocol (CoAP), failed to provide solutions and, therefore, foster IoT network availability.

Denial-of-Service attacks obstruct the communication between devices and prevent them for accessing network resources. According to [114], 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 Distributed Denial-of-Service (DDoS) attacks as well. DoS attacks against IoT systems, as exposed by [115], 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. [105, p. 649] states that DDoS are “particularly severe” for IoT systems constituted of vulnerable nodes from a network layer standpoint. [114] defines 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, critical for constrained devices [117]. Physical damage, as stated by [115], can also be considered a DoS threat executed by less knowledgeable attackers to cripple IoT services by “things” destruction.

[117] defines DDoS attacks as the set of concurrent DoS attacks. Therefore, the authors suggest in their work, a Service Oriented Architecture (SOA) as a DDoS prevention strategy for IoT systems. Traditional approaches to prevent DoS or DDoS attacks rely on heavy network traffic sampling, [117] proposes an optimized solution based on random sampling and sampling rate efficiency. [114] lists various DoS defense techniques for WSN including [118], [103] and [107]. Nevertheless, the authors indicate that there is not an existing defense mechanism capable of ruling out DoS risks. DoS attack detection is very difficult to accomplish, according to [114], since the symptoms of such attacks may also make some services unavailable. [114], proposes an Intrusion-Detection-System (IDS) 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 [115] suggest the implementation of distributed architectures instead of centralized approaches. One of the main advantages portrait 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. [105] stress on the importance of disaster recovering procedures to be placed after large-scale or elaborated DDoS attacks.

D. Privacy

The significant growth of the IoT has showed during recent years has brought in several privacy concerns as data availability soars, sponsored by ubiquitous and pervasive properties of the IoT [85] [119], and the fact that devices at the moment do not offer all the desired warranties. [24] calls for protection of users’ personal information associated to their “movements, habits and interactions” [24, 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 [25] [4], harming as well the possibility for widespread adoption of IoT technologies [4] [85] [120]. [87] discusses worst-case scenarios and undesirable situations produced by “Big Brother-like entities” [87, p. 54] where data is collected and shared without user consent.

[121] distinguishes 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 & governance, as well as policy implementation and management. [87] also proposes solutions to the IoT privacy problems, the first one is to provide “privacy by design” [87, 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 [119]. [10] also includes Transparency as a privacy solution, as it allows users to know the parties that manage and utilize the data collected by a IoT device. [119] proposes Data Management as a solution as well, composed by the implementation of differentiated policies and enforcing instruments. [119] also discusses the necessity for data typification as well as ownership, access extent (minimum and maximum of data to be read), anonymity and its viability. [4] proposes the implementation of opt-out features managed by individuals wherever an untrustworthy sensor network has been implemented, also called “right to silence of the chips” [16, p. 26], as well the interaction with a “privacy broker” [122] that acts as a proxy between the user and the network. [120] indicates that technological solutions are not enough to address the current privacy issues and calls for the consideration of economical and socio-ethic aspects of the IoT environment. [115] includes as well the revision of the existing privacy regulations at the private and government level as well as improving the users’ awareness on how sensor-based devices collect, store and share their information. However, it is not that simple as stated by [123] as the re-classification and distinction between regular and Personal Identifiable Information (PII), which can be protected by law, for IoT devices is still a challenge to overcome. [16] questions 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 boundaries and jurisdictions. Nevertheless, government entities, such as the European Commission and the US Federal Communications Commission (FCC) [10],

have already called for recommendations in the deployment of sensor networks as well as the collaboration within the civil society stakeholders for the creation of a privacy framework that works at different levels.

VI. 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 Internet of Things relay, each one of them provides significant value to the whole system. These segmentation provides 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.

The IoT, then, needs a deeper discussion that strengthens its foundations towards 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.

VII. CONCLUSION

The ongoing Internet of Things state reveals that there is still significant work to do 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 last 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 continue 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. Final 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.

REFERENCES

- [1] Gartner, “Gartner says 6.4 billion connected “things” will be in use in 2016, up 30 percent from 2015.” <http://www.gartner.com/newsroom/id/3165317>. [Online; accessed 06-December-2016].
- [2] Forbes, “152,000 smart devices every minute in 2025: Idc outlines the future of smart things.” <http://www.forbes.com/sites/michaelkanellos/2016/03/03/152000-smart-devices-every-minute-in-2025-idc-outlines-the-future-of-smart-things/#34bf983369a7>. [Online; accessed 06-December-2016].
- [3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.
- [4] L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” *Computer Networks*, vol. 54, no. 15, pp. 2787 – 2805, 2010.
- [5] K. Zhao and L. Ge, “A survey on the internet of things security,” in *Computational Intelligence and Security (CIS), 2013 9th International Conference on*, pp. 663–667, IEEE, 2013.
- [6] M. Weyrich and C. Ebert, “Reference architectures for the internet of things,” *IEEE Software*, vol. 33, no. 1, pp. 112–116, 2016.
- [7] P. Adolphs, H. Bedenbender, D. Dirzus, M. Ehlich, U. Epple, M. Hankel, R. Heidel, M. Hoffmeister, H. Huhle, B. Kärcher, et al., “Reference architecture model industrie 4.0 (rami4. 0),” *ZVEI and VDI, Status Report*, 2015.
- [8] I. I. Consortium et al., “Industrial internet reference architecture,” *Industrial Internet Consortium, Tech. Rep., June*, 2015.
- [9] A. B. HEU, P. G. HEU, A. O. CEA, and J. Stefa, “Internet of things architecture,” 2013.
- [10] R. H. Weber, “Internet of things: Privacy issues revisited,” *Computer Law & Security Review*, vol. 31, no. 5, pp. 618–627, 2015.
- [11] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, “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, IEEE, 2012.
- [12] H. Ning and Z. Wang, “Future internet of things architecture: like mankind neural system or social organization framework?,” *IEEE Communications Letters*, vol. 15, no. 4, pp. 461–463, 2011.
- [13] K. on Security, “Ddos on dyn impacts twitter, spotify, reddit,” 2016.
- [14] W. of Science Thomson Reuters, “Web of science [v.5.21] - all databases.” <https://webofknowledge.com>. [Online; accessed 04-December-2016].
- [15] E. Borgia, “The internet of things vision: Key features, applications and open issues,” *Computer Communications*, vol. 54, pp. 1–31, 2014.
- [16] R. H. Weber, “Internet of things—new security and privacy challenges,” *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, 2010.
- [17] F. Zafari, I. Papapanagiotou, and K. Christidis, “Micro-location for internet of things equipped smart buildings,” *CoRR*, vol. abs/1501.01539, 2015.
- [18] F. Zafari, I. Papapanagiotou, and K. Christidis, “Microlocation for internet-of-things-equipped smart buildings,” *IEEE Internet of Things Journal*, vol. 3, pp. 96–112, Feb 2016.
- [19] A. Ukil, J. Sen, and S. Koilakonda, “Embedded security for internet of things,” in *Emerging Trends and Applications in Computer Science (NCETACS), 2011 2nd National Conference on*, pp. 1–6, IEEE, 2011.

- [20] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," 2016.
- [21] A. W. Atamli and A. Martin, "Threat-based security analysis for the internet of things," in *Secure Internet of Things (SIoT), 2014 International Workshop on*, pp. 35–43, IEEE, 2014.
- [22] D. Boyle and T. Newe, "Securing wireless sensor networks: security architectures," *Journal of networks*, vol. 3, no. 1, pp. 65–77, 2008.
- [23] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of security and privacy issues of internet of things," *arXiv preprint arXiv:1501.02211*, 2015.
- [24] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.
- [25] C. M. Medaglia and A. Serbanati, "An overview of privacy and security issues in the internet of things," in *The Internet of Things*, pp. 389–395, Springer, 2010.
- [26] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *Security in pervasive computing*, pp. 201–212, Springer, 2004.
- [27] D. Henrici and P. Müller, "Tackling security and privacy issues in radio frequency identification devices," in *International Conference on Pervasive Computing*, pp. 219–224, Springer, 2004.
- [28] E. B. Kavun and T. Yalcin, "A lightweight implementation of keccak hash function for radio-frequency identification applications," in *International Workshop on Radio Frequency Identification: Security and Privacy Issues*, pp. 258–269, Springer, 2010.
- [29] T. Phillips, T. Karygiannis, and R. Kuhn, "Security standards for the rfid market," *IEEE Security & Privacy*, vol. 3, no. 6, pp. 85–89, 2005.
- [30] D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc networks," *IEEE communications surveys*, vol. 7, no. 4, pp. 2–28, 2005.
- [31] T. Naeem and K.-K. Loo, "Common security issues and challenges in wireless sensor networks and iee 802.11 wireless mesh networks," *3; 1*, 2009.
- [32] "Status of project iee 802.11ah." http://www.ieee802.org/11/Reports/tgah_update.htm. Accessed: 2016-08-09.
- [33] L. Costantino, N. Buonaccorsi, C. Cicconetti, and R. Mambrini, "Performance analysis of an lte gateway for the iot," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a*, pp. 1–6, IEEE, 2012.
- [34] I. Bilogrevic, M. Jadliwala, and J.-P. Hubaux, "Security issues in next generation mobile networks: Lte and femtocells," in *2nd international femtocell workshop*, no. EPFL-POSTER-149153, 2010.
- [35] I. Papapanagiotou, D. Toumpakaris, J. Lee, and M. Devetsikiotis, "A survey on next generation mobile wimax networks: objectives, features and technical challenges," *Communications Surveys & Tutorials, IEEE*, vol. 11, no. 4, pp. 3–18, 2009.
- [36] S. S. Hasan and M. A. Qadeer, "Security concerns in wimax," in *Internet, 2009. AH-ICI 2009. First Asian Himalayas International Conference on*, pp. 1–5, IEEE, 2009.
- [37] M. Bogdanoski, P. Latkoski, A. Risteski, and B. Popovski, "Ieee 802.16 security issues: A survey," 2008.
- [38] P. Rengaraju, C.-H. Lung, Y. Qu, and A. Srinivasan, "Analysis on mobile wimax security," in *Science and Technology for Humanity (TIC-STH), 2009 IEEE Toronto International Conference*, pp. 439–444, IEEE, 2009.
- [39] C.-T. Huang and J. M. Chang, "Responding to security issues in wimax networks," *IT Professional*, vol. 10, no. 5, pp. 15–21, 2008.
- [40] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger, "Nfc devices: Security and privacy," in *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*, pp. 642–647, IEEE, 2008.
- [41] K. Curran, A. Millar, and C. Mc Garvey, "Near field communication," *International Journal of Electrical and Computer Engineering*, vol. 2, no. 3, p. 371, 2012.
- [42] H. Eun, H. Lee, and H. Oh, "Conditional privacy preserving security protocol for nfc applications," *Consumer Electronics, IEEE Transactions on*, vol. 59, pp. 153–160, February 2013.
- [43] Estimote, "Estimote real world context for your apps." <http://www.estimote.com/>. [Online; accessed 26-Sept-2014].
- [44] R. Bouhenguel, I. Mahgoub, and M. Ilyas, "Bluetooth security in wearable computing applications," in *2008 International Symposium on High Capacity Optical Networks and Enabling Technologies*, pp. 182–186, IEEE, 2008.
- [45] A. Sharma, "Bluetooth security issues: threats and consequences," in *Proc. of the 2nd national conference COIT*, pp. 78–80, Citeseer, 2008.
- [46] D. K. Oka, T. Furue, L. Langenhop, and T. Nishimura, "Survey of vehicle iot bluetooth devices," in *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, pp. 260–264, IEEE, 2014.
- [47] I. S. Bayram and I. Papapanagiotou, "A survey on communication technologies and requirements for internet of electric vehicles," *EURASIP Journal on Wireless Communications and Networking*, vol. 2014, p. 223, Dec 2014.
- [48] F. Zafari and I. Papapanagiotou, "Enhancing ibeacon based micro-location with particle filtering," in *Global Communications Conference (GLOBECOM), 2015 IEEE*, pp. 1–7, IEEE, 2015.
- [49] F. Zafari, I. Papapanagiotou, T. Hacker, and M. Devetsikiotis, "Enhancing the accuracy of ibeacons for indoor proximity-based services," in *International Communications Conference (ICC), 2017 IEEE*, May 2017.
- [50] F. Zafari, I. Papapanagiotou, M. Devetsikiotis, and T. J. Hacker, "An ibeacon based proximity and indoor localization system," *CoRR*, vol. abs/1703.07876, 2017.
- [51] N. A. Dudhane and S. T. Pitambare, "Location based and contextual services using bluetooth beacons: New way to enhance customer experience," *Lecture Notes on Information Theory Vol*, vol. 3, no. 1, 2015.
- [52] Z. Alliance, "Zigbee security specification overview," 2006.
- [53] N. Vidgren, K. Haataja, J. L. Patino-Andres, J. J. Ramirez-Sanchis, and P. Toivanen, "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, IEEE, 2013.
- [54] M. Knight, "Wireless security-how safe is z-wave?," *Computing & Control Engineering Journal*, vol. 17, no. 6, pp. 18–23, 2006.
- [55] B. Fouladi and S. Ghanoun, "Security evaluation of the z-wave wireless protocol," *Black hat USA*, vol. 24, 2013.
- [56] D. Trends, "Z-wave just made your smart home devices safer via a new security protocol." <https://www.digitaltrends.com/home/z-wave-security-protocol/>. [Online; accessed 06-May-2017].
- [57] Z.-W. Alliance, "Z-wave alliance announces new security requirements for all z-wave certified iot devices."
- [58] S. Ullah, M. Ali, A. Hussain, and K. S. Kwak, "Applications of uwb technology," *arXiv preprint arXiv:0911.1681*, 2009.
- [59] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. Mccann, and K. Leung, "A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities," *Wireless Communications, IEEE*, vol. 20, no. 6, pp. 91–98, 2013.
- [60] S. Park *et al.*, "Ipv6 over low power wpan security analysis draft-glowpan-security-analysis-05," tech. rep., IETF Internet Draft, 2011.
- [61] M. A. Razaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for internet of things: a survey," *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 70–95, 2016.
- [62] P. R. Pietzuch, *Hermes: A scalable event-based middleware*. PhD thesis, University of Cambridge, 2004.
- [63] M. Eisenhauer, P. Rosengren, and P. Antolin, "Hydra: A development platform for integrating wireless devices and sensors into ambient intelligence systems," in *The Internet of Things*, pp. 367–373, Springer, 2010.
- [64] D. Guinard, V. Trifa, S. Karnouskos, P. Spiess, and D. Savio, "Interacting with the soa-based internet of things: Discovery, query, selection, and on-demand provisioning of web services," *IEEE transactions on Services Computing*, vol. 3, no. 3, pp. 223–235, 2010.
- [65] M. Caporuscio, P.-G. Raverdy, and V. Issarny, "ubisoap: A service-oriented middleware for ubiquitous networking," *IEEE Transactions on Services Computing*, vol. 5, no. 1, pp. 86–98, 2012.
- [66] C.-L. Fok, G.-C. Roman, and C. Lu, "Servilla: A flexible service provisioning middleware for heterogeneous sensor networks," *Science of Computer Programming*, vol. 77, no. 6, pp. 663–684, 2012.
- [67] I. Corredor, J. F. Martínez, M. S. Familiar, and L. López, "Knowledge-aware and service-oriented middleware for deploying pervasive services," *Journal of Network and Computer Applications*, vol. 35, no. 2, pp. 562–576, 2012.
- [68] Xively, "Xively by logmein: Iot platform for connected devices." <https://www.xively.com/>. [Online; accessed 16-January-2017].
- [69] S. Satyadevan, B. S. Kalarickal, and M. Jinesh, "Security, trust and implementation limitations of prominent iot platforms," in *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*, pp. 85–95, Springer, 2015.
- [70] Carriots, "Carriots - internet of things platform." <https://www.carriots.com/>. [Online; accessed 16-January-2017].
- [71] Echelon, "Echelon - home." <http://www.echelon.com/>. [Online; accessed 16-January-2017].

- [72] N. Costa, A. Pereira, and C. Serodio, "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. 50–50, IEEE, 2007.
- [73] M. Nagy, A. Katasonov, M. Szydowski, O. Khriyenko, S. Nikitin, and V. Terziyan, *Challenges of middleware for the internet of things*. INTECH Open Access Publisher, 2009.
- [74] A. L. Murphy, G. P. Picco, and G.-C. Roman, "Lime: A middleware for physical and logical mobility," in *Distributed Computing Systems, 2001. 21st International Conference on*, pp. 524–533, IEEE, 2001.
- [75] C. Curino, M. Giani, M. Giorgetta, A. Giusti, A. L. Murphy, and G. P. Picco, "Mobile data collection in sensor networks: The tinylime middleware," *Pervasive and Mobile Computing*, vol. 1, no. 4, pp. 446–469, 2005.
- [76] R. d. C. A. Lima, N. S. Rosa, and I. R. L. Marques, "Ts-mid: 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, IEEE, 2008.
- [77] K. Aberer, M. Hauswirth, and A. Salehi, "A middleware for fast and flexible sensor network deployment," in *Proceedings of the 32nd international conference on Very large data bases*, pp. 1199–1202, VLDB Endowment, 2006.
- [78] D. Zhao and I. Raicu, "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, IEEE, 2013.
- [79] U. of California Berkeley, "Tinydb: A declarative database for sensor networks." <http://telegraph.cs.berkeley.edu/tinydb/>. [Online; accessed 16-January-2017].
- [80] A. N. A. Stanford-Clark, "Mqtt version 3.1. 1," *OASIS Std.*, October, 2014.
- [81] R. Neisse, G. Steri, and G. Baldini, "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, IEEE, 2014.
- [82] M. Singh, M. Rajan, V. Shivraj, and P. Balamuralidhar, "Secure mqtt for internet of things (iot)," in *Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on*, pp. 746–751, IEEE, 2015.
- [83] P. Saint-Andre, "Extensible messaging and presence protocol (xmpp): Core," 2011.
- [84] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
- [85] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.
- [86] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," *Wireless Personal Communications*, vol. 58, no. 1, pp. 49–69, 2011.
- [87] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *Computer*, vol. 44, no. 9, pp. 51–58, 2011.
- [88] L. Zhou and H.-C. Chao, "Multimedia traffic security architecture for the internet of things," *Network, IEEE*, vol. 25, no. 3, pp. 35–40, 2011.
- [89] S. Hong, D. Kim, M. Ha, S. Bae, S. J. Park, W. Jung, and J.-E. Kim, "Snaill: an ip-based wireless sensor network approach to the internet of things," *Wireless Communications, IEEE*, vol. 17, no. 6, pp. 34–42, 2010.
- [90] D. Zuehlke, "Smartfactorytowards a factory-of-things," *Annual Reviews in Control*, vol. 34, no. 1, pp. 129–138, 2010.
- [91] A. C. Sarma and J. Girão, "Identities in the future internet of things," *Wireless personal communications*, vol. 49, no. 3, pp. 353–363, 2009.
- [92] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, "Key management systems for sensor networks in the context of the internet of things," *Computers & Electrical Engineering*, vol. 37, no. 2, pp. 147–159, 2011.
- [93] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for internet of things," *Journal of network and computer applications*, vol. 42, pp. 120–134, 2014.
- [94] C. P. Mayer, "Security and privacy challenges in the internet of things," *Electronic Communications of the EASST*, vol. 17, 2009.
- [95] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security challenges in the ip-based internet of things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 527–542, 2011.
- [96] A. Singla, A. Mudgerikar, I. Papapanagiotou, and A. A. Yavuz, "Haa: Hardware-accelerated authentication for internet of things in mission critical vehicular networks," in *Military Communications Conference, MILCOM 2015 - 2015 IEEE*, pp. 1298–1304, Oct 2015.
- [97] A. Singla, A. Mudgerikar, I. Papapanagiotou, and A. Yavuz, "Fast and scalable authentication for vehicular internet of things," in *Proceedings of the 16th Annual Information Security Symposium, CERIAS '15*, (West Lafayette, IN), pp. 22:1–22:1, CERIAS - Purdue University, 2015.
- [98] A. A. Yavuz, A. Mudgerikar, A. Singla, I. Papapanagiotou, and E. Bertino, "Real-time digital signatures for time-critical networks," *IEEE Transactions on Information Forensics and Security*, vol. PP, no. 99, pp. 1–1, 2017.
- [99] R. Acharya and K. Asha, "Data integrity and intrusion detection in wireless sensor networks," in *Networks, 2008. ICON 2008. 16th IEEE International Conference on*, pp. 1–5, IEEE, 2008.
- [100] D. Christin, A. Reinhardt, P. S. Mogre, and R. Steinmetz, "Wireless sensor networks and the internet of things: selected challenges," *Proceedings of the 8th GI/ITG KuVS Fachgespräch Drahtlose Sensornetze*, pp. 31–34, 2009.
- [101] D. Uckelmann, M. Harrison, and F. Michahelles, *An architectural approach towards the future internet of things*. Springer, 2011.
- [102] T. Tsao, R. Alexander, M. Dohler, V. Daza, and A. Lozano, "A security framework for routing over low power and lossy networks," *raft-ietf-roll-security-framework-05 (work in progress)*, 2011.
- [103] O. Garcia-Morchon, R. Hummen, S. Kumar, R. Struik, and S. Keoh, "Security considerations in the ip-based internet of things, draft-garcia-core-security-04," 2012.
- [104] S. Alam, M. M. Chowdhury, and J. Noll, "Interoperability of security-enabled internet of things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 567–586, 2011.
- [105] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, vol. 3, pp. 648–651, IEEE, 2012.
- [106] J. Mineraud, O. Mazhelis, X. Su, and S. Tarkoma, "A gap analysis of internet-of-things platforms," *arXiv preprint arXiv:1502.01181*, 2015.
- [107] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security challenges in the ip-based internet of things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 527–542, 2011.
- [108] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "Twenty security considerations for cloud-supported internet of things," 2015.
- [109] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "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, IEEE, 2011.
- [110] L. Coetzee and J. Eksteen, "The internet of things-promise for the future? an introduction," in *IST-Africa Conference Proceedings, 2011*, pp. 1–9, IEEE, 2011.
- [111] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *Proceedings of the 52nd Annual Design Automation Conference*, p. 54, ACM, 2015.
- [112] A. Fongen, "Identity management and integrity protection in the internet of things," in *2012 Third International Conference on Emerging Security Technologies*, pp. 111–114, IEEE, 2012.
- [113] H. C. Van Tilborg and S. Jajodia, *Encyclopedia of cryptography and security*. Springer Science & Business Media, 2014.
- [114] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-service detection in 6lowpan based internet of things," in *2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 600–607, IEEE, 2013.
- [115] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.
- [116] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *Communications Surveys & Tutorials, IEEE*, vol. 17, no. 4, pp. 2347–2376, 2015.
- [117] S. Misra, P. V. Krishna, H. Agarwal, A. Saxena, and M. S. Obaidat, "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, IEEE, 2011.
- [118] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," *Pervasive Computing, IEEE*, vol. 7, no. 1, pp. 74–81, 2008.
- [119] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, 2014.
- [120] L. Tan and N. Wang, "Future internet: The internet of things," in *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, vol. 5, pp. V5–376, IEEE, 2010.

- [121] O. Vermesan and P. Friess, *Internet of things: converging technologies for smart environments and integrated ecosystems*. River Publishers, 2013.
- [122] G. V. Lioudakis, E. A. Koutsoloukas, N. Dellas, S. Kapellaki, G. N. Prezerakos, D. I. Kaklamani, and I. S. Venieris, "A proxy for privacy: the discreet box," in *EUROCON, 2007. The International Conference on &# 34; Computer as a Tool&# 34;*, pp. 966–973, IEEE, 2007.
- [123] S. R. Peppet, "Regulating the internet of things: First steps toward managing discrimination, privacy, security and consent," *Tex. L. Rev.*, vol. 93, p. 85, 2014.