Manas Ranjan Moharana *et al*, International Journal of Computer Science and Mobile Applications,
National Conference on "The Things Services and Applications of Internet of Things",
Gandhi Institute for Education and Technology (GIET) Baniatangi, 23-24 March 2018, pg. 113-121
ISSN: 2321-8363
Impact Factor: 5.515

THE CURRENT STATE AND SECURITY ASPECTS OF IOT

Manas Ranjan Moharana[1], Ranjita Rout[2]

[1]*Department of Computer Science & Engineering, GIET, Baniatangi, BBSR, ranjan01.manas@gmail.com*
[2] *Department of Computer Science & Engineering, GIET, Baniatangi, BBSR, rout.ranjita@gmail.com*

Abstract
The Internet of Things (IoT) is a network of physical objects connected to internet over a specified path for effective monitoring of physical objects. Physical objects embedded with RFID, sensor and so on which allows object to communicate with each other. These physical objects are provided with unique identifier to make its unique identity. As the IoT is highly dynamic and heterogeneous, security is a major challenge in IoT. In this paper we analyzed the different security requirements and challenges in IoT and other research parameters. This paper is a general survey of all the security issues existing in the Internet of Things (IoT) along with an analysis of the privacy issues that an end-user may face as a consequence of the spread of IoT. The majority of the survey is focused on the security loopholes arising out of the information exchange technologies used in Internet of Things

Keywords: Security, RFID, WSN, Privacy, Denial Of Service

I. Introduction
The Internet of Things (IoT) is a concept that describes the fact where the daily used activities and components can be connected to the Internet and also be able to identify themselves to other devices . IoT is closely identified with RFID, sensor technologies, wireless technologies. It allows objects to be sensed and controlled remotely across existing network infrastructure maintaining proper connection among the devices. The internet is a medium that connect people across the world with the help of computing device for emailing, gaming, conferencing, online trading and so on. This techniques can also be used in the purposes like controlling physical devices . This technique can be considered as the Things and services of internet of things(IoT). The IoT can be able to transfer data over the network without human interaction. The need of the Internet of Things (IoT) is the concept of every device blending with the existence of human beings. It is the state where there is no difference between the operation of devices surrounding us and our actions. There is a continuous integration between us and the "things" around our surrounding. The different 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 Zetta bytes 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

ISSN: 2321-8363
Impact Factor: 5.515

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 technologies and protocols, discusses the IoT security concerns and explores the current privacy issues of IoT systems under different points of view. Finally, concludes with the content to give a clear idea about the perception of the ongoing security challenges of the IoT and overlays some solutions.

II. STRUCTURE OF IOT SYSTEMS

The IoT is a heterogeneous, dynamics, intelligence, mobility and undefined parameters makes it a high demand technology domain but also makes the IoT vulnerable and risky under security terms. The different platform 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 a more important parameter of concern.

The foundation for computing, whose goal is to connect everyday life objects to the network using technology, is made up of three basic 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

The IoT architecture, is composed of three layers

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

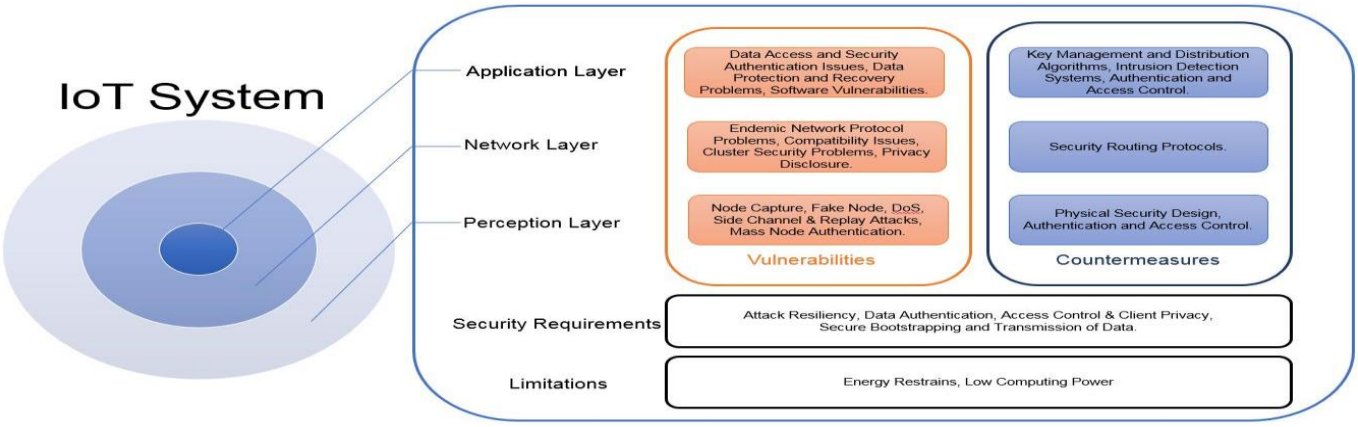

Fig. 1. Internet of Things Security Landscape

ISSN: 2321-8363
Impact Factor: 5.515

The perception layer gathers environmental data, the network layer, which is composed of wired and wireless systems processes and transmits the input obtained by the perception layer supported by technological platforms. The application layer consists of abstracted solutions that interact with the final users in order to satisfy their needs. The IoT requires architectural solutions that can manage heterogeneous states in order to work efficiently and effectively [6]. Figure 1 summarizes current IoT architecture frameworks/standards and highlights their security objectives. Architecture and model implementation helps IoT developers to focus and structure their efforts on users' require-ments, 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. 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

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 modules include the following components:

( ) Hardware

(a) Communication stack

(b) Middleware

(c) Secure data Aggregation

Similar to active Radio Frequency Identification (RFID) technology, the data collected by the sensor nodes is shared between them or by a centralized system for analytic purposes [3].

ISSN: 2321-8363
Impact Factor: 5.515

A WSN is composed of the following elements:

(a) Sensor

(b) Micro-controller

(c) Memory

(d) Radio transceiver

(e) Battery

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 set-tings. 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].

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 fulfil 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

ISSN: 2321-8363
Impact Factor: 5.515

also vulnerable to tampering as attackers may found them easier to access that 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].

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' sub layer [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.

Near Field Communication: Near Field Communication (NFC) has a short range of 20 centimetres; 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.

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 hoping, (2) Restricted

ISSN: 2321-8363
Impact Factor: 5.515

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 micro location purposes through beacons enabled by Bluetooth Low Energy (BLE) technology [48],or proximity applications [50]. BLE communication is confirmed 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].

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].

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

ISSN: 2321-8363
Impact Factor: 5.515

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 net-works. 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.

D. 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.

E. 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 senders 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.

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

ISSN: 2321-8363
Impact Factor: 5.515

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 fulfil their requirements under strict control and scrutiny to manage the always present risk for inter-connectivity.

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] 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.

[3] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787 – 2805, 2010.

[4] 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.
[5] M. Weyrich and C. Ebert, "Reference architectures for the internet of things," IEEE Software, vol. 33, no. 1, pp. 112–116, 2016.

[6] P. Adolphs, H. Bedenbender, D. Dirzus, M. Ehlich, U. Epple, M. Han-kel, R. Heidel, M. Hoffmeister, H. Huhle, B. Karcher," et al., "Reference architecture model industrie 4.0 (rami4. 0)," ZVEI and VDI, Status Report, 2015.

[7] I. I. Consortium et al., "Industrial internet reference architecture," Industrial Internet Consortium, Tech. Rep., June, 2015.
[8] A. B. HEU, P. G. HEU, A. O. CEA, and J. Stefa, "Internet of things architecture," 2013.
[9] R. H. Weber, "Internet of things: Privacy issues revisited," Computer Law & Security Review, vol. 31, no. 5, pp. 618–627, 2015.

[10] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the in-ternet of things architecture, possible applications and key challenges," in Frontiers of Information Technology (FIT), 2012 10th International Conference on, pp. 257–260, IEEE, 2012.

[11] 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.

[12] K. on Security, "Ddos on dyn impacts twitter, spotify, reddit," 2016.

[13] W. of Science Thomson Reuters, "Web of science [v.5.21] - all databases." https://webofknowledge.com. [Online; accessed 04-December-2016].
[14] E. Borgia, "The internet of things vision: Key features, applications and open issues," Computer Communications, vol. 54, pp. 1–31, 2014.

[15] R. H. Weber, "Internet of things–new security and privacy challenges," Computer Law & Security Review, vol. 26, no. 1, pp. 23–30, 2010.

[16] F. Zafari, I. Papapanagiotou, and K. Christidis, "Micro-location for in-ternet of things equipped smart buildings," CoRR, vol. abs/1501.01539, 2015.
[17] 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.
[18] 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. Fernandez, 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.

ISSN: 2321-8363
Impact Factor: 5.515

[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. Muller, "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 In-ternational 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 ieee 802.11 wireless mesh networks," 3; 1, 2009.

[32] "Status of project ieee 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] 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 Transac-tions 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 tech-nologies and requirements for internet of electric vehicles," EURASIP Journal on Wireless Communications and Networking, vol. 2014, 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, "En-hancing 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.

