SECURITY AND PRIVACY ISSUES IN INTERNET OF THINGS

Zahraddeen Gwarzo

PhD Candidate, Oakland University, Department of Computer Science and Engineering
2200 N.Squirrel Road, Rochester, MI-48309, US
zhgwarzo@oakland.edu

Keywords: ***Security, Internet of Things, Objects, Privacy, Cryptography, Authentication, Standardization, Access control***

Abstract: *The growing ambition to connect every «thing» to the internet, and provide a platform on which these «things» talk to one another has become an irresistible drive. Objects, Humans, Animals, Service Providers, Processing Systems and Intelligent Systems make up the Internet of things. The security and privacy challenges in such a vast extension of our powers into unknown territory are enormous. Weak authentication mechanisms due to constrained resources, lack of effective access control, lack of physical security over the proliferation of «objects», and privacy issues we had never contemplated before, are all now first coming to light.*

1. Introduction

We are currently witnessing the evolution and proliferation of a pervasive paradigm called «The internet of things». IoT as it is often referred to, is comprised of several technologies, including the traditional internet, radio frequency identification (RFID) systems, wireless sensor networks (WSNs), machine-to-machine platforms, big data, cloud services, and smart applications, among other things. It is estimated, that over fifty billion devices will be connected to the internet by the year 2020 [1].

With the capability of IPv6 addressing to accommodate 2^128 devices, every «thing» on the planet can uniquely connect to the IoT. The IoT has the purpose of providing an IT based infrastructure thereby facilitating the exchange of «things» in a reliable and secure manner [2].

The reader should realize that IoT is such a complex paradigm that stakeholders need to address several issues associated with it, among which are Security, Privacy, Scalability, Standardization, and so on. In addition to the existing conventional attacks such as man-in-the-middle attack, denial of service attack, identity theft, IP spoofing, among other things, we may witness a new wave of attacks such as hackers controlling and or destroying/damaging IoT objects in homes, hospitals, airports, among other environments. Other attacks similar to conventional attacks such as worms' propagation in the IoT, virus attacks etc. could be devastating. Generally, the threats in the IoT network are similar to those of the traditional network. However, the wider impact can be very different.

This paper reviews important security and privacy issues discussed in the literature. The rest of the paper is organized as follows. Section 2 gives a background concept of internet of things. Section 3 discusses the main security and privacy issues surrounding key components of IoT including RFID systems, Sensor nodes, and consumer devices. Section 4 discusses the security and privacy issues of the two main architectures of IoT; Centralized versus Distributed approaches. Section 5 discusses Network layer security issues in IoT. Section 6 briefly discusses Application Layer Security Issues. Section 7 discusses some views of the main IoT stakeholders with regards to the security challenges that lie ahead. Section 8 concludes the paper.

2. Background

Although there is no one universal definition of the IoT, the concept is unique and universal. Things such as physical objects, people and even animals would be connected to the internet and provided with the framework and the capability to talk to one another. In a nutshell, the vision of IoT is to connect every physical object on the planet to the Internet. These objects will be given a unique identifier such as an IP address. It is estimated that the IoT will have 30 billion devices connected wirelessly to the internet by the year 2020 [3], and Ericsson predicts it will be more than 50 billion devices [4].

As the internet of Things evolves rapidly, it is expected to offer advanced connectivity among devices, systems and services which would go beyond machine-to machine (M2M) communications and cover a variety of protocols, domains and applications [5]. Wireless Sensor Networks (WSNs) and Radio Frequency Identification (RFID) are the current forecast of the Internet of Things with respect to devices connectivity and service portability. An enormous amount of research is going on today in the field of Internet of Things. Many stakeholders such as governments, researchers, and IT professionals among others have been attracted by this technological revolution. Unfortunately, the Internet of things is currently being developed without appropriate consideration of security challenges and regulation [6]. This paper studies thoroughly the security issues of IoT that were discussed in the literature and presents them in the following sections.

3. Issues in IoT Devices

3.1. Vulnerabilities in IoT Devices

It is estimated that IoT will have more than 30 billion devices connected by the year 2020. Most of these IoT devices will have some security vulnerabilities. The research conducted by Hewlett Packard (HP) indicated that 70 percent of the 10 most popular IoT devices such as TVs, webcams, garage door openers, sprinkler controllers, and home thermostats, among other things, contain massive vulnerabilities. These vulnerabilities include weak passwords, heartbleed (vulnerability in the OpenSSL cryptographic software library enabling hackers to steal information), denial of service and Cross Site Scripting, among other things [7]. The research reveals five major issues associated with these devices as follows:

Privacy Issues. The research reveals that 80% of the devices raise privacy concerns. For example, many devices collect some kind of personal information; names, addresses, credit card numbers, health information and date of birth. And the most dangerous thing is the fact that many of these devices transmit data over the network in clear text, i.e unencrypted. The study has also discovered that most of the tested IoT devices use cloud services which have many security issues themselves (such as the issue of Trust) making these IoT devises more vulnerable.

Insufficient Authentication and Authorization. The research study also reveals that 80% of the tested IoT devices do not have strong password requirements, with most allowing weak passwords such as «1234». With issues like this, it is obvious that an attacker can take advantage of such vulnerability to gain access to the device in question.

Lack of Transport Encryption. The research study also reveals that 70% of the devices do not encrypt communications to the internet and the local network. Encrypting network services that transmit data via the internet and the local network is crucial in protecting the confidentiality and integrity of the transmitted information, and most importantly in the context of IoT, given the amount of information that is being passed between the devices, the cloud and mobile applications.

Insecure Web Interface. The research study further shows that 60% of the devices tested reveal security

issues with their web interface, including persistent cross-site scripting, poor session management and weak default credentials.

Insecure Software and Firmware. Sixty percent of the devices tested do not use encryption when downloading software updates. The research claims to have demonstrated the interception of some of the downloads, extracted, and mounted as file system in Linux where the software can be viewed or modified. This development is really worrying as billions of devices are poised to be part of the IoT.

3.2. RFID and WSN Security

Although a wide range of devices, networks and service technologies will make up the IoT, RFID is seen as key among the technologies that will make IoT a reality [8–12]. As billions of physical objects are poised to connect to the internet in the IoT paradigm, they also aim to communicate with one another. Consequently, data and information representation, storage, organization, and transmission will be extremely challenging [13]. As challenging as data and information handling will be in IoT, the security will be at least as complicated.

Before going into the security issues associated with RFID and WSNs, it is worth taking a brief look at the background of these two important players in the IoT. The RFID system is composed of, from a few to tons of tags, one or more readers, one or more antennas associated with each reader, and a central or distributed server(s) that manages the readers. RFID tags are attached to an object (anything; from computing devices to grocery products to human beings and animals) in order to uniquely identify and track such an object with accuracy and automation as opposed to an optical barcode. An RFID tag is small in size, and usually passive (although there are also active and semi passive RFID tags), which means that they do not have a power source; they harvest power from the signal of an interrogating reader [14].

On the other hand, WSNs are active, and since communication is peer to peer, WSNs do not need the presence of a reader. A WSN is comprised of sensing nodes and usually a node referred to as a Sink, which receives data from the other nodes' activities. WSNs are mostly based on IEEE 802.15 standard which is designed for low constraint devices in a Wireless Personal Area Network (WPAN). WSNs are currently used in several applications, such as healthcare, smart environment, smart building, and military applications among other things. Using WSNs in collaboration with RFID systems in an IoT will help in facilitating more efficient communication and tracking of objects. Several proprietary and non-proprietary technologies are currently used for WSNs, such as ZigBee, Z-Wave, and Wavenis, among others. Details of these technologies are beyond the scope of this paper. However, the interested reader can find more details about these technologies in [15–19]

Poor Authentication and Authorization. Security implementations of most RFID tags and Sensor nodes (which are low cost) are currently not good enough to prevent attack. This is attributable to their low computational capabilities. Each RFID tag has a unique identifier which points to database entries consisting of very private and secure information about an object such as transaction histories, shopping habit, address of a person and even credit card information, among other things. Weak authentication and authorization mechanisms can lead to total compromise of the IoT system. Therefore, strong encryption algorithms and other cryptographic techniques for the purpose of effective **authentication** such as public key cryptography cannot be implemented in these low cost constrained devices. Currently, light encryption is applied on these devices. This is far from being the solution.

Physical Security. Sensor nodes and RFID tags are mostly idle as such an attacker can physically damage them. A more skillful attacker may attempt to perform reverse engineering on these devices.

Privacy Issues and the Concept of Anonymity. As certain tags carry personal information such as financial, medical and other sensitive information, the possibility of covert tracking and inventorying of tags by unauthorized readers that are within range is very real. Information transmitted form authorized readers to the tag can be eavesdropped within a relatively long distance of hundreds of meters. Therefore, user centric support such as allowing IoT users to retain their **anonymity** is very important. However, the majority of users are not experts and as such they do not really understand how to make the necessary user centric configurations. Effective implementation of privacy by design principles was addressed in [20**].** Privacy by design emphasize the need to embed privacy right from the beginning, during the architecture, design and construction of processes, because of the possibility of powerful analytics to make it possible to re-identify individuals (after de-identifying them) over huge dataset.

Authors of [21] use Daidalo's virtual identity concept [22] to propose an identity-based personal location system with protected privacy in the IoT. The model is designed to protect users' location and information from unauthorized other users. The model uses multiple unassociated unique virtual identities (VID) for a user for different roles. Each VID is used in different services in order to conceal the ***location identity*** of the user who may be a patient. The system is comprised of Registration management authority (RMA) which is a trusted entity that registers and provides users with VIDs, a system which authenticates users based on their VIDs, a Policy system which stores and updates relevant policies to ensure user anonymity, and a client system which keeps copies of user VIDs on the user's mobile device for the purpose of communication with the server. The system authenticates users using their VIDs. The policy system further ensures that no two VIDs (for different roles) belonging to a single user can ever be linked to one another thereby preserving the privacy of such a user. While this is a good privacy model, however, it may be less useful in accident emergency situations at least in the developed world, since there is a more efficient way of handling accident emergency situations. Similar approaches can be seen in [23–24].

4. Centralized vs Distributed IoT

4.1. Centralized IoT

Many IoT solutions such as Thingworx, Xively, and ARM, among others, adopt a centralized IoT architecture using cloud based technologies to deliver IoT services to their customers. The idea of a centralized IoT is to provide the edge network with the platform on which the edge objects will be sending their data to the central entity for storage and processing. Third parties can create their own IoT applications through the Application Programming Interfaces (APIs) that are provided by the central entity. In a nutshell, in a centralized IoT, the intelligence lies at the central entity as opposed to a distributed IoT. However, the scalability of objects and resources that the IoT requires is beyond a centralized data collection and centralized objects management. It will be very inefficient to manage millions of objects or collect data from scarce resources centrally as such the need to bring the intelligence to the edge network i.e. closer to the objects. This is called distributed intelligence, distributed computing or Fog computing.

4.2. Distributed IoT

A distributed system is a collection of independent computers that appears to its users as a single coherent system [25]. Similarly, in a distributed IoT, several entities which make up the IoT appear to their users as one single entity. Communications can go both ways, and unlike in a centralized IoT architecture, entities can actually receive data from other entities (located in different context) and execute them. The intelligence is shifted to the edge network. This means, that objects can acquire, process data, and make decisions as needed. A daunting task ahead, imagine the volume of data, that will be flowing within a distributed IoT, where entities

have to interpret the data and make important decisions. Issues ranging from the role of middleware (an integral part of traditional distributed systems) in a distributed IoT, to impact of hardware and software failures, and communication channels, are well beyond the scope of this paper. However, the interested reader can refer to [26–28] for more understanding on the challenges that lie ahead in a distributed IoT.

As billions of things in multiple contexts are poised to connect to the IoT and to one another, it is crucial that authentication and authorization of these connecting objects and entities are as effective as that of the traditional networks. We need to preserve the integrity and confidentiality of the huge volume of data, that would be flowing. It is challenging to implement proper authentication and authorization mechanisms necessary for the security and privacy of the entities and the data being exchanged between these heterogeneous objects and entities [29].

4.3. Security and Privacy issues

The internet of things will be an ocean of objects and other entities. Lack of security protocols standardization and the absence of a unified security solution introduce many security and privacy issues in the IoT. Issues ranging from effective identification, authentication and authorization of «things» to the implementation, storage and management of access control policies, to privacy safeguards and trust issues are all very much a concern to security professionals and business experts.

Authentication and Authorization. An authentication mechanism is relatively easy to implement in a centralized IoT since the implementation is done at a central entity/location. However, it will be challenging to implement and manage authentication and authorization in a distributed IoT because of the scalability, manageability and multiple context issues associated with the «things» that are being authenticated. The number of «things» joining IoT networks periodically would be enormous as such it will be challenging to identify and authenticate «things» that are joining for the first time, for example, potentially malicious «things». It is important if not crucial that the acquisition and processing of sensitive/private information such as health data is owned and controlled by the relevant users themselves. This may be achieved by the use of tokens (objects which represent the right to perform an operation). Whenever the relevant information needs to be acquired and processed, the system notifies the relevant user which in turn grants or denies the tokens which will be used to authenticate the end user and the process.

OpenID [30] is a framework that facilitates authentication and authorization based on explicit user privacy control. However, this framework is restricted to http which is not ideal for the IoT. Other alternative protocols more suitable for the IoT such as MQTT, XMPP, COAP, DDS, and AMQP are discussed in the Protocols Standardization section below.

Access Control. Effective access control is crucial to the success of IoT security. The implementation and management of access control in a distributed IoT environment is far from being simple or straight forward. Access control policies would be simpler to create and manage in a centralized IoT than in a distributed IoT. However, Privacy issues arise when access control policies are applied in a distributed IoT, where «things» cannot control who accesses their data and information. Existing traditional access control approaches may not be easy to implement in a distributed IoT environment. One reason is, storing the list of users and their access rights will not be effective because of the scalability and manageability issues associated with the distributed IoT environment.

A more promising approach is Capability Role Based Access Control (CapBAC) which is devised according to the capability based authorization model [31]. In this approach, a capability, which is basically an authorization token, is used to uniquely refer to an object or entity along with the entity's specific access rights. So any process that needs to interact with an object has to acquire the capability token associated with the object. And

the most interesting part of this approach is that, it is the object owner that grants and ascertains its authorization capability to the service provider, unlike in a traditional access control system where the reverse is the case.

Protocols Standardization. IoT will have several different security and communication protocols. While some of these protocols may be compatible with each other, others would not be. For example, ZigBee, an IEEE 802.15.4 communication protocol, which is popular with the IoT, uses security methods that utilize AES-128 bit encryption standard and in some instances Elliptic Curve Cryptography (ECC) certificate based methods [32]. Another IoT wireless communication protocol; Z-Wave, uses a different security method although also AES-128 bit encryption standard like some of ZigBee's methods, however, the two are not compatible [32]. Different vendors, hundreds of millions of things, different communication channels and protocols, how do we start looking for security vulnerabilities? But we will have to collectively find a solution capable of tackling this problem.

Although the five main IoT messaging protocols (MQTT, XMPP, DDS, COAP and AMQP) have recently been standardized, a few of the several different implementations of each have been standardized. For example, MQTT (Message Queue Telemetry Transport) is a lightweight simple messaging protocol designed for constrained objects and networks with significant overhead [33], has only version 3.1.1 of its implementations standardized. Besides, IoT needs many more protocols apart from these five [34–35], and the process of standardization can take several years. What we are more concerned here, is how secure are these communication protocols? The design principle of these protocols is more of performance and reliability with little or no emphasis on security. MQTT is intended to be light and simple and was not designed to handle a strong authentication process, making it insecure by itself.

Constrained Application Protocol (COAP) works like HTTP as a web transfer protocol but for constrained devices unlike HTTP which is not a lightweight protocol. COAP is built without appropriate security considerations and is susceptible to spoofing attacks, among other things.

Data Distribution Service (DDS) distributes data between devices, making it a device to device protocol. It provides scalability, performance, and Quality of Service required to support IoT applications. DDS may be the most promising among the IoT protocols. It has an advanced security implementation which provides standardized authentication, encryption, access control and logging capabilities to enable secure data connectivity between end to end DDS compliant devices in the IoT system [36].

It is important to remember that many of the security considerations for IoT protocols are dependent on encryption and hence there is a need to adopt encryption algorithm(s) that are suitable for the IoT objects. In 2012, SHA-3 algorithm was selected by the National Institute of Standards and Technology (NIST) as the standard algorithm for the smart devices [37]. Security breaches go for the weakest link, and that is why standardization is very important!

Privacy Safeguards and Trust. We pointed out in the Authentication and Authorization section above, the importance of having the acquisition and processing of sensitive data (such as health data) owned and controlled by the relevant users/patients themselves. It is crucial to make sure that patients (owners of the health devices) are involved in every stage of this process such that no tokens are issued without the explicit approval of the patient. We believe a mechanism like this one will not only protect user's privacy but ensure ***trust*** among the IoT actors. In order to achieve trust between entities, entities need to authenticate each other as proposed in [38].

Constrained Resources. As we have discussed in section 3.2 (Poor Authentication and Authorization), most of IoT entities suffer from limited resources such as battery power, memory and processing power. This limitation greatly affects the implementation of strong authentication mechanism for these constrained objects

in the IoT. A good solution to the limited resources of the «things», at least for now, would be to introduce a mechanism that would delegate «trust» to the connecting Gateways, which are normally powerful and can handle very strong cryptographic encryption.

5. IoT Network Security

Although security at the network layer has been strengthened over the years, IoT faces similar threats as traditional networks. Because communication among IoT devices is mainly wireless, attacks such as Man-in-the-middle, Denial of Service, and Eavesdropping, among other things, can be perpetrated relatively easily as such these attacks are very much a threat in the IoT as well. A scenario of a Man-in-the-middle attack in an IoT is illustrated in [39], where a node in IoT is utilized as an identification and authentication mechanism for some services based on RFID. An attacker could deploy transceivers very close to the server node and the client nodes. All communication coming from the server node would be intercepted by the nearby transceiver and then relayed to the client nodes. Similarly, communications coming back from the client nodes would be intercepted by the transceiver and then relayed to the server node thus deceiving both the client nodes and the server node into establishing trust with the transceiver and authenticating it to have whatever service the client node was requesting. And it did not matter whether the communication was encrypted or not. Figure 1 illustrates this scenario.

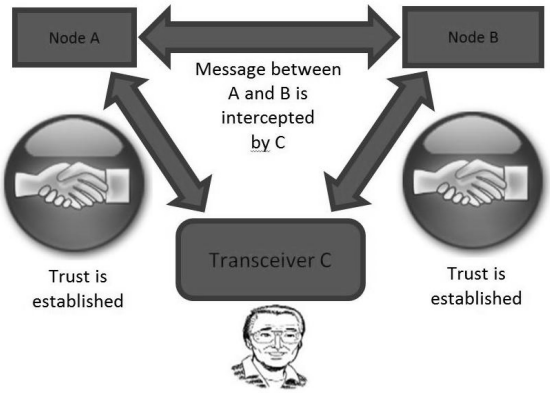

Figure 1. Man-in-the-Middle attack scenario

Recall in section 3.1 above, the research conducted by HP indicated that 70 percent of the IoT devices tested failed to encrypt communication at the transport level. This meant that communications over the local network or to the internet travel in clear text, making it easy for an attacker to intercept and even modify them, as such data confidentiality and integrity are a serious concern in the IoT. It is worth noting that the solution would be to enforce a strong encryption policy, but key components of IoT, such as the devices, sensors, and the RFID tags among other things, all have low computational capability and low memory and energy consumption capacity and hence cannot handle strong authentication mechanisms. Therefore continued research in this domain is very much needed.

Because of the passive nature of IoT, authentication mechanisms using centralized architectures are only useful in a centralized IoT where a central entity (such as an application based on a cloud service) stores, processes and manages information. This scenario is not the case in a distributed IoT as data providers (e.g. sensors, RFID tags etc.) can acquire and process data and information from different entities. The best solution would be to embed strong cryptographic encryption and access control at the object level. Again, the computational

and power limitations of these objects leave the field for research wide open.

6. IoT Applications Security

IoT applications such as smart transportation, health, environmental monitoring, assisted driving, military applications, among other things, are truly making the IoT phenomenon pervasive and ubiquitous. However, there are security issues with these applications, e.g. as follows:

Consider the situation of a medical patient whose health condition is being monitored by a smart health system. This can be achieved by attaching RFID tags and sensors to the body of this patient. These IoT devises will be reporting and communicating with the smart health system about the condition of the patient, and the smart health application will store and process the patient's information. Therefore, data confidentiality and integrity must be ensured to prevent data leakage and loss. As small IoT networks merge into large IoT networks, IoT objects will try to access data and security issues arise. Therefore, proper **access control** and **authentication mechanisms** that define who can access what must be implemented. It would be difficult to implement effective access control in IoT as discussed in section 4.3.

7. Views of IoT stakeholders

SANS Institute [40] published a survey in 2014 in which it wanted to find out what the security community thought about the current and future realities of IoT. So it posted a survey for security personnel that are active in the IT field.

There is some good and some bad news about the findings. Security professionals recognize that existing security controls are insufficient for the complex IoT, are already dealing with a number of interconnected things and are planning for the emergence of more complex devices. The survey indicates that most responders (90%) believe that, in order to secure IoT, existing security controls have to be changed with some foreseeing nearly complete enhancement and replacement of existing security controls. The survey further indicates that security professionals are concerned with the capabilities of internet connected computing of medical devices, smart buildings and industrial control systems in an IoT set up.

8. Conclusion

There are serious and so far unaddressed issues in the IoT. The security and privacy challenges facing the emerging IoT paradigm are enormous. From an army of heterogeneous and ubiquitous devices and objects, to massive network traffic, to weak authentication mechanisms for resource constrained objects, to ineffective access control for the scalable and dynamic IoT, to physical security of passive and pervasive objects. Therefore, continued research in all the layers of communication is crucial. Current security controls cannot provide the needed security for the IoT, as such security professionals must continue to analyze existing and future security architectures in order to prepare for the security challenges of this dynamic paradigm called the «Internet of Things». Researchers must develop an efficient and flexible IoT security framework capable of addressing the enormous security challenges of IoT.

9. References

[1] Sundmaeker, Harald/Guillemin, Patrick/Friess, Peter/Woelfflé, Sylvie, Vision and challenges for realising the Internet of Things. *CERP-IoT, European Commission-Information Society and Media*, Brussels 2010, p. 3.

[2] Floerkemeier, Christian/Langheinrich, Marc/Fleish, Elgar/Mattern, Friedmann/Sarma, Sanjay E. (Eds.), The Internet of Things: First International Conference, IoT 2008, Zurich, Switzerland, March 26–28, 2008, Proceedings. Vol. 4952. Springer Science & Business Media, Berlin, Heidelberg 2008.

[3] ABI research, More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020. *ABI research news*, https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne/ (last accessed on 3 February 2016) 2013.

[4] Kushalnagar, Nandakishore/Montenegro, Gabriel/Christian, Schumacher, IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals. *RFC4919*, IETF Trust 2007.

[5] Holler, Jan/Tsiatsis, Vlasios/Mulligan, Catherine/Avesand, Stefan/Karnouskos, Stamatis/Boyle, David, From Machine-to-machine to the Internet of Things: Introduction to a New Age of Intelligence. Academic Press, Massachusette 2014, pp. 30–32.

[6] Clearfield, Chris, Why The FTC Can't Regulate The Internet Of Things, Forbes/Tech, http://www.forbes.com/sites/chrisclearfield/2013/09/18/why-the-ftc-cant-regulate-the-internet-of-things/#4665bb7853ae (last accessed on 3 February 2016) 2013.

[7] HP. Fortify on Demand. Internet of Things Research Study, *HP Report*, http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf (last accessed on 17 January 2016) 2014.

[8] Presser, Mirko/Gluhak, Alexander, The Internet of Things: Connecting the Real World with the Digital World. *EURESCOM mess@ ge – The Magazine for Telecom Insiders 2*, 2009.

[9] Zorzi, Michele/Gluhak, Alexander/Lange, Sebastian/Bassi, Alessandro, From today's intranet of things to a future internet of things: a wireless-and mobility-related view. *Wireless Communications*, IEEE 17, no. 6, 2010, pp. 44–51.

[10] Welbourne, Evan/Battle, Leilani/Cole, Gregory/Gould, Kyle/Rector, Kyle/Raymer, Samuel/Balazinska, Magdalena/Borriello, Gaetano, Building the internet of things using RFID: the RFID ecosystem experience. *Internet Computing*, IEEE 13, no. 3, 2009, pp. 48–55.

[11] Khoo, Benjamin. RFID as an enabler of the internet of things: issues of security and privacy. *Internet of Things (iThings/CPSCom)*, 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing. IEEE, 2011, pp. 709–712.

[12] Trotter, Matthew, RFID Makes Internet of Things Come to Life, machine design, http://machinedesign.com/iot/rfid-makes-internet-things-come-life (accessed on 21 September 2015), 2014.

[13] Katasonov, Artem/Kaykova, Olena/Khriyenko, Oleksiy/Nikitin, Sergiy/Terziyan, Vagan, Smart Semantic Middleware for the Internet of Things. *ICINCO-ICSO 8*, 2008, pp. 169–178.

[14] Juels, Ari, RFID security and privacy: A research survey. *Selected Areas in Communications*, IEEE Journal on 24.2, 2006, pp. 381–394.

[15] Mainetti, Luca/Patrono, Luigi/Vilei, Antonio, Evolution of wireless sensor networks towards the internet of things: A survey. *Software, Telecommunications and Computer Networks (SoftCOM)*, 2011 19th International Conference on. IEEE, 2011, pp. 1–6.

[16] Yick, Jennifer/Mukherjee, Biswanath/Ghosal, Dipak, Wireless sensor network survey. *Computer networks* 52.12 (2008), pp. 2292–2330.

[17] Gomez, Carles/Paradells, Josep, Wireless home automation networks: A survey of architectures and technologies. *IEEE Communications Magazine* 48.6 (2010), pp. 92–101.

[18] Baronti, Paolo/Pillai, Prashant/Chook, Vince/Chessa, Stefano/Gotta, Alberto/Hu, Y. Fun, Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards. *Computer communications* 30, no. 7 (2007), pp. 1655–1695.

[19] Lee, Jin-Shyan/Su, Yu-Wei/Shen, Chung-Chou, A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. *Industrial Electronics Society*, 2007. IECON 2007. 33rd Annual Conference of the IEEE. IEEE, 2007.

[20] Cavoukian, Ann/Jonas, Jeff, Privacy by design in the age of big data, Information and Privacy Commissioner of Ontario, Canada, 2012.

[21] Hu, Chunye/Zhang, Jie/Wen, Qiaoyan An identity-based personal location system with protected privacy in IoT. *Broadband Network and Multimedia Technology (IC-BNMT)*, 2011 4th IEEE International Conference on. IEEE, 2011.

[22] Daidalos' Projects, http://www.ist-daidalos.org/daten/publications/EU-leaflet/EU-project_Daidalos_II_Summary.pdf (last accessed on 28 November 2015).

[23] Sarma, Amardeo C./Girão, João, Identities in the future internet of things. *Wireless personal communications* 49.3

(2009), pp. 353–363.

[24] Sarma, Amardeo/Matos, Alfredo/Girão, João/Aguiar, Rui, Virtual identity framework for telecom infrastructures. *Wireless Personal Communications* 45, no. 4 (2008), pp. 521–543.

[25] Tanenbaum, Andrew S./Van Steen, Maarten, Distributed systems, Prentice-Hall, Upper Saddle River, NJ 2007.

[26] Masri, Wassim/Mammeri, Zoubir, Middleware for wireless sensor networks: A comparative analysis. *Network and Parallel Computing Workshops*, 2007. NPC Workshops. IFIP International Conference on. IEEE, 2007, pp. 349–356.

[27] Ibrahim, Noha, Orthogonal classification of middleware technologies. *Mobile Ubiquitous Computing, Systems, Services and Technologies*, 2009. UBICOMM'09. Third International Conference on. IEEE, 2009, pp. 46–51

[28] Charles, John, Middleware moves to the forefront. *Computer 5*, 1999, pp. 17–19.

[29] Uckelmann, Dieter/Harrison, Mark/Michahelles, Florian, Architecting the internet of things. Springer Science & Business Media, Berlin Heidelberg 2011, pp. 1–24.

[30] OpenID, OpenID Connect, http://openid.net/connect/ (last accessed on 5 December 2015).

[31] Gusmeroli, Sergio/Piccione, Salvatore/Rotondi, Domenico, A capability-based security approach to manage access control in the internet of things. *Mathematical and Computer Modelling* 58.5 (2013): 1189–1205.

[32] Wrote an e-mail to Zigbee support team at help@zigbee.org and got this reply answered by their certificate and technology team on 23 November 2015.

[33] MQTT, http://mqtt.org/faq (last accessed on 2 December 2015).

[34] Wu, Miao/Lu, Ting-lie/Ling, Fei-Yang/Sun, Ling/Du, Hui-Ying, Research on the architecture of Internet of things. *Advanced Computer Theory and Engineering (ICACTE)*, 2010 3rd International Conference on, vol. 5, pp. V5-484. IEEE, 2010.

[35] Schneider, Stan, Understanding the Protocols Behind the Internet of Things, http://electronicdesign.com/iot/understanding-protocols-behind-internet-things (last accessed on 2 February 2016) 2013.

[36] DDS, Why Choose DDS, http://portals.omg.org/dds/why-choose-dds/ (last accessed on 7 December 2015).

[37] Boutin, Chad, NIST Selects Winner Of Secure Hash Algorithm (SHA-3) Competetion, http://www.nist.gov/itl/csd/sha-100212.cfm (last accessed on 7 December 2015), 2012.

[38] Mahalle, Parikshit/Babar, Sachin/Prasad, Neeli/Prasad, Ramjee, Identity management framework towards internet of things (IoT): Roadmap and key challenges. *Recent Trends in Network Security and Applications*, pp. 430–439. Springer Berlin Heidelberg, 2010.

[39] Atzori, Luigi/Iera, Antonio/Morabito, Giacomo, The internet of things: A survey. *Computer networks* 54.15 (2010): 2787–2805.

[40] SANS Institute, InfoSec Reading Room, Securing the Internet of Things Survey, http://www.sans.org/reading-room/whitepapers/analyst/securing-internet-things-survey-34785 (last accessed on 27 April 2015).