Towards Security Solutions in IoT Sensor Network and Middleware

A Systematic mapping

Cícero Woshington Saraiva Leite
FJN-Faculdade de Juazeiro do Norte
Juazeiro do Norte, Brasil
email:cicerow.ordb@gmail.com

Leonardo Lourenço Lacerda
CESAR-Centro de Estudos e Sistemas Avançados do Recife
Maceió, Brasil
email:leonardolacerda.as@gmail.com

Fábio Lucas Faleiro Naves
CESAR-Centro de Estudos e Sistemas Avançados do Recife
Iporá, Brasil
email:fabionaves@gmail.com

Cícero Samuel Clemente Rodrigues
FJN-Faculdade de Juazeiro do Norte
Juazeiro do Norte, Brasil
email:samuelclerod@gmail.com

Geiziany Mendes da Silva
FJN-Faculdade de Juazeiro do Norte
Juazeiro do Norte, Brasil
email:geiziany.mendes@gmail.com

Abstract — Internet of Things (IoT) is present in several environments, from houses to large health care institutions. Data flows from small sensors and actuators to large data centers and cloud computer services. Small sensors and actuators need to guarantee data confidentiality, availability and integrity, even with limited resources. This paper presents a systematic mapping outlining problems and solutions studied in the last three years about middleware and sensors network security. The process used to select, filter and analyze articles is described and the results indicate efforts to certify integrity, availability and, especially, confidentiality.

IoT; Middleware; Sensor Network.

I. INTRODUCTION

The term Internet of Things (IoT) was first proposed in 1999, in an article of the RFID Journal, when a supply chain was interconnected with an enterprise using Radio Frequency Identification (RFID) [1]. According to Khan, an IoT environment has to promote connectivity with everything and everyone [2], through a group of interconnected sensors, providing a set of relevant information for a computer decision support system.

According to Business Insider, almost $6 trillion must be invested in solutions using IoT in the next five years [24]. IoT is one emergent technology in Gartner's IT Hype Cycle [3], as seen in Fig. 1.

In the last years, concepts about IoT have been implemented in many sectors, such as health care, public services, transport and so forth. This paradigm of interconnected things increases the challenge to develop and maintain an infrastructure to assist this demand without security problems.

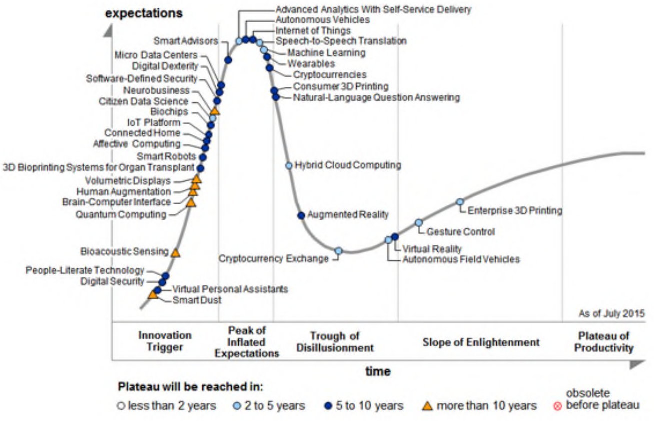

Figure 1. Gartner's IT Hype Cycle [3]

An architecture proposed by Tan and Wang (2010) and Wu et al. split the components used in IoT environments in 5 layers: perception (device), transport, processing (middleware), application and business [4]. This work will focus on the perception, transport and processing layers of this model.

Every computing system may have security problems and the same can be said about IoT. A secure computing system has to guarantee the following pre-requisites:

- Availability: related to the computing system's level of availability.
- Integrity: related to the guarantee that information was not modified in its source or on its path.
- Confidentiality: related to the assurance that only an authorized person can access the data.

ISBN: 978-1-61208-505-0

In IoT, the perception layer is mainly composed of sensors, which are small, autonomous, with low processing and low power consumption [5]. These features, combined with its wide dispersion, make it even more complex to guarantee privacy and security to the information collected without the considerable increase in power consumption and processing in these wireless sensor networks [6].

This work intends to do a systematic mapping of problems and solutions in security communication within sensor networks and middleware used in IoT environments between devices in the perception and processing layers. According to Petersen (2008), systematic mapping involves a search in literature to verify the nature, extension and quantity of published articles [7]. IoT was the object of multiple studies over the last years and this work has the purpose of identifying and categorizing problems and solutions related to sensor networks and middleware security in IoT, resulting in a reference to related studies.

This work is organized in five sections: Section 2 presents the theoretical principles of IoT, its concepts and components. After that, Section 3 explains the process used in systematic mapping detailing the process of search. It also specifies the academic databases included in the research and the criteria for their inclusion and exclusion. Moreover, Section 4 analyzes and classifies the data collected and, finally, Section 5 presents the conclusion of this work.

II. THEORETICAL PRINCIPLES

A. Internet of Things (IoT)

IoT is a model that uses several objects (or things) to establish a pervasive presence around us [9]. These objects are present in houses, offices, industries, etc., providing information about the context where they work [10]. Applications use the Internet to consume such information and to serve reasoning and semantic data, intelligent and responsive services, big data analysis, and so on. Thus, a network of objects, services and people is ordered. Atzori et al. show the interaction of these elements, as shown in Fig. 2 [9].

The top circle in Fig. 2 lists some of the objects used in an IoT environment. Almost all of these objects are small electronic sensors and actuators capable of interacting with the real environment. Nonetheless, there are many technologies to develop and to implant these objects. The technologies shown in Fig. 2 are only a short enumeration.

Usually, sensors and actuators have a small amount of resources to process or store data (even none). Some of these sensors are integrated with smartphones and other small computing platforms (like Arduino and Raspberry PI). Finally, all these objects need a way to connect to the Internet moving from the top circle to the left circle. Sometimes, middlewares are necessary to assure the compatibility of elements. Sensors, actuators and communication devices cover mold, what is called "things" oriented vision [9]. The initial efforts to implant IoT platforms over the years were concentrated in the top circle elements and there are plenty of technologies in the market about this.

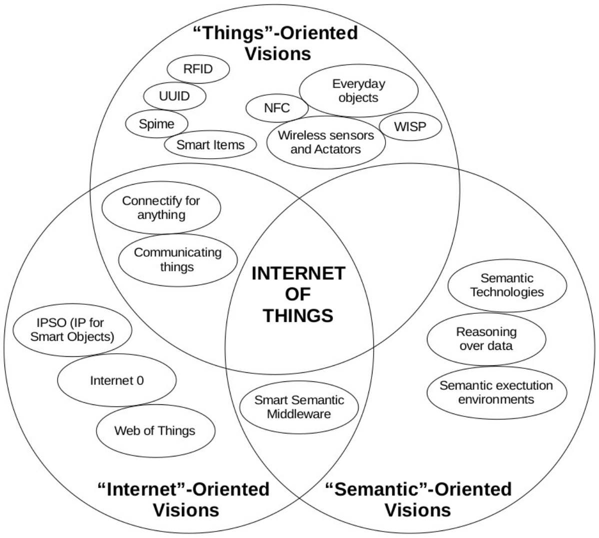
"Things"-Oriented Visions
RFID
UUID
Spime
Smart Items
NFC
Everyday objects
WISP
Wireless sensors and Actators
Connectify for anything
Communicating things
INTERNET OF THINGS
IPSO (IP for Smart Objects)
Internet 0
Web of Things
Smart Semantic Middleware
Semantic Technologies
Reasoning over data
Semantic exectution environments
"Internet"-Oriented Visions
"Semantic"-Oriented Visions

Figure 2. "Internet of Things" paradigm as result of the convergence of different visions [9].

Nowadays, another concept is being studied. Quantum Lifecycle Management (QLM) messaging is a standard based on IoT that defines changes in a life cycle of information between different IoT products [11].

The left circle in Fig. 2 presents some technologies used to provide applications that interact with objects, such as those presented in the top circle. The "Internet"-oriented vision is the connection between humans and objects in the IoT concept. Humans, using a computer or a smart device, can receive a data summary from sensors and send commands to the actuators.

There is another modern approach to understand this part of the concept. For example, Guo et al. present the opportunistic IoT to provide networks compatible with the movement and opportunistic contact of the human nature. Then, a person who interacts with an environment of objects (sensors and actuators) will find other people to provide the network to share and feed the applications used in the left circle [11]. Thus, smart mobile devices connected in ad-hoc networks are the center of this concept to reflect the human-human interaction against the human-computer interaction reflected in network layout. Therewith, the IoT environment will reproduce the human behavior more than objects behavior, changing and improving the context of information.

Moving to the right circle, the applications designed to interact with humans have to interact with other applications to extend their capability. The elements called Web of Things (WoT) must implement new interfaces to computers over the network or Internet. Again, new middleware is necessary to exchange data between these elements. Some technologies, such as Simple Object Access Protocol (SOAP) or Representational State Transfer (REST), are examples in this case. REST is a lightweight integration technology introduced in 2000 by Roy Fielding. Rettig et al. present a research work in which REST is applied in this context [13].

Finally, in the right circle, the analysis of the data collected and processed in the left circle will provide some new real time information. At this stage, the analysis will focus on providing knowledge more than information. The objective is not to understand the responses of sensors, but to interpret this information comparing it with another environment with the same context or even to compare it with other contexts to create new knowledge about this. According to Atzori et al., to represent, store, interconnect, search and organize the magnitude of information generated by so many devices will be a great challenge [9].

B. *Middlewares*

Rocha et al. affirm that distributed systems generate new problems because they are not centralized. Among the questions regarding distributed systems is: how to make it easy the development of distributed systems and the integration with legacy systems? One of the responses to this question is middlewares [14].

Maciel et al. (2004) define middleware as a software layer that permits communication between distributed applications. In other words, middlewares are responsible for interoperating between systems, providing a layer to allow transparent communication, minimizing complexity and providing a homogeneous environment for the few or several systems that might be involved [15].

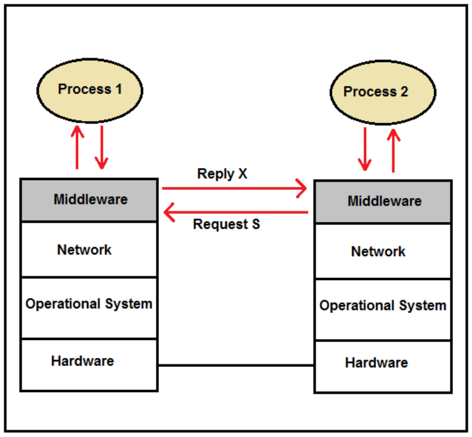

Figure 3. Communication between middleware [15].

Fig. 3 shows a usage example of a middleware. The middleware layer is inside the structure and it is responsible for providing communication between existent systems. The process is transparent to the applications (processes 1 and 2) and the middleware handles the communication in a heterogeneous environment.

According to Cavalcanti et al., the main middleware features are [16]:

- Hiding the information distributed.
- Hiding the hardware components heterogeneity from several operating systems and communication protocols.
- Providing high-level uniform interfaces to applications and developers.
- Supplying a set of common services to execute some general functions, avoiding effort duplication and facilitating collaboration between applications.

Middleware is gaining market over the past years in order to integrate legacy systems with new systems and also to simplify the integration by developing new services to both systems.

Nowadays, middleware is used in several scenarios, including IoT, from e-health to smart houses where middleware is responsible for providing communication between some sensors and interoperating them with other systems.

C. *Sensors Networks*

When the Internet was proposed, the objective was to create a long distance decentralized communication network. The client/server paradigm suggests an application with one human interacting directly, with a client side and one computer at the server side.

Despite this, sensor networks designed for an IoT environment involve communication between a sensor and a transport device without a human being in the circuit. These components are installed at a short distance in the same environment for almost all cases. Finally, sensors, actuators and transport devices have reduced capacity to store and process data and it is difficult to connect the sensor network to the Internet because the data from the sensors cannot be transmitted in long distance with the limitation of these transmission protocols. With low power of processing data, even none, sensors are not able to execute complex algorithms to cypher information [17].

In this scenario, to ensure security features, especially confidentiality, can be a great challenge. Many different studies try to solve this problem with diverse approaches: “small sized keys, reduce communication exchanges, operate under the assumption of insecure communication channels, etc.” [18], but the discussion along this work shows the challenge is only in its beginning. To face various different scenarios, with singular needs and features, using distinct technologies and implementing particular sets of protocols is necessary to stablish more solutions with different cost/benefit relations. This justifies the relevance of the systematic mapping conducted to understand the most recent studies about this topic.

III. SYSTEMATIC MAPPING

The systematic mapping adopted in this work is based on the process proposed by Petersen et al. (2008) that describes five steps [7]:

1. Research questions definitions;
2. Primarily relevant studies research;
3. Classification (first filter);
4. Summary keyword (second filter);
5. Data extraction and mapping.

Usually, questions in a systematic mapping must be general, of an exploratory nature, while systematic revisions may use more specific questions [8]. This way, this work focuses on the following questions:

- (Q1). Which are the main problems related to communication security in sensors network and middleware used in IoT?
- (Q2). Which are the solutions to communication security in sensors network and middleware used in IoT?

The academic databases chosen to be part of this research were ACM Digital Library, Elsevier (Science Direct) and IEEE Xplore. The elected research keywords were: IoT, security and sensors networks. To classify the articles, the following criteria for inclusion were established:

- Articles from 2014 or newer;
- For articles about the same research subject, only the most recent were selected;

Exclusion criteria were:

- Any article about other subjects, not analyzed in this paper;
- Secondary studies such as summary, presentations and so forth;

The first search returned a total of 649 papers. The first filter (reading the titles and abstracts in order to apply inclusion and exclusion criteria) reduced the number of articles to 94. The second filter (reading the introductions) reduced the number to 60 after we applied applied again the inclusion and exclusion criteria. The result is presented in Table I.

TABLE I. ARTICLES NUMBERS

BASE	First Filter	Second Filter	Final Selection
ACM Digital Library	199	42	24
Elsevier (Science Direct)	222	22	12
IEEE Xplore	225	30	24
Total	646	94	60

To answer the first question (Q1) the articles were arranged in groups: Confidentiality, Availability, Integrity and ALL, presented in Section 1 of this paper. To resolve the second question (Q2), the articles were classified according to the presented solution:

- Cryptography – key generator: key generation solutions;
- Cryptography – key management: key management and distribution solutions;
- Anonymity: guarantees privacy solutions;
- Internal prevention of attacks: prevents attacks from devices inside sensor network;
- Architecture: proposed architecture to implant security;
- Physical attack: physical attacks to devices, for instance to steal or to break;
- Authentication: guarantees both, identity and source of information;

IV. ANALYSIS

This section presents details about the study and the collected information during the classifying process. Fig. 4 shows the relation between academic databases and the articles classified. The analysis draws 24 (39,7%) articles from ACM, 24 (39,7%) from IEEE Xplore and 12 (20,7%) from Elsevier.

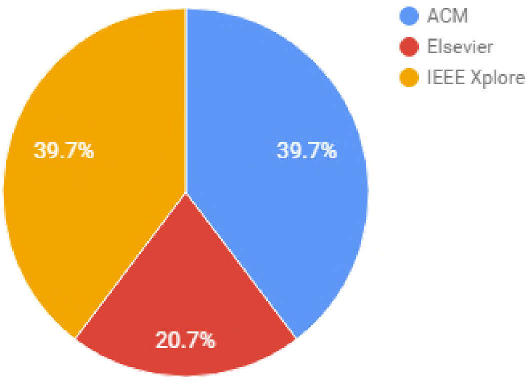

Figure 4. Counts of Base

In all the articles included, 60% enumerate confidentiality as the main problem to be solved by security middlewares in sensor networks in an IoT environment. As proposed by Baker (2009 apud Ntul et al. 2016) [19], capturing data or doing a physical attack in a sensor network means that “the attacker can clone the device, install new firmware or learn sensitive information”. The hacked device might be used in other complex and destructive attacks. Belsis and Pantziou [20], Gope and Hwang [21], and others show the risk of intercepting and infering data about patients and location in a medical monitoring environment in a likely IoT approach. Something between sensors and gateways must assure the privacy of people and accuracy of the health information. It can be applied to other environments. Caron et al. [22] discuss the privacy to the Australian citizen and the legal guarantees to protect personal information. The center of the discussion features how secrecy, anonymity and solitude can be applied to almost every country in the modern world. Nonetheless, low cost devices have limited processing power and have to use simple cryptographic and sign functions [23]. Fig. 5 shows the percentage of distribution of security problems of this study.

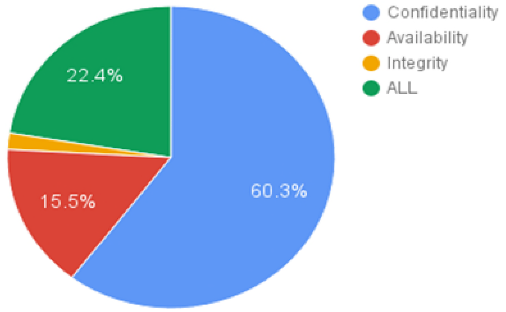

Figure 5. Percentage of security problems

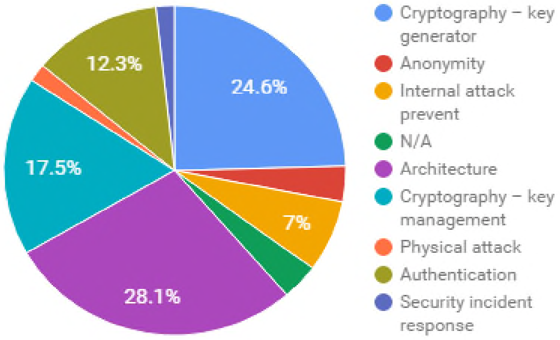

Figure 6. Percentage of security solutions

Among the identified problems, a few proposed solutions were identified. Those were arranged in categories. Fig. 6 represents the distribution of categories for solutions and percentage from the selected articles.

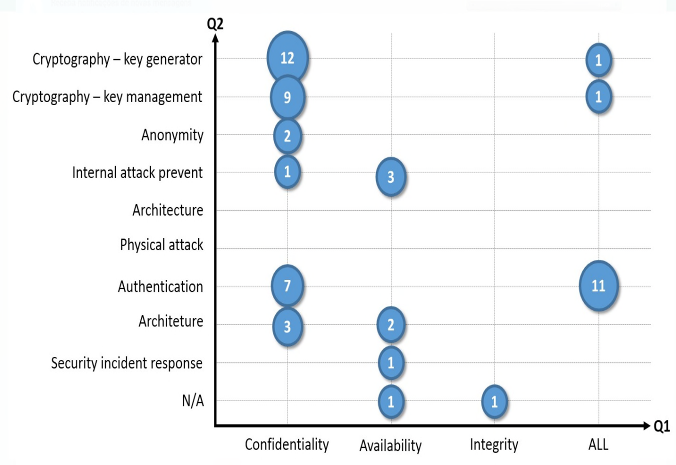

Figure 7. Mapping

The main concerns found about the solutions were: Cryptography - Key Management (17.5%), Cryptography - Key Generator (24.6%) and Architecture (28.1%). These represent 70,2% of all solutions found. Solutions based in Architecture represent 28.1%, but solutions based in Cryptography are more recurring representing 45,6%, almost half of all solutions. About the Architecture category, many solutions were proposed, such as network architecture to middleware model, including specific security issues with focus in data confidentiality and integrity. The N/A category groups articles without proposed solutions. Fig. 7 shows the articles distribution comparing the two questions: problems (Q1) and proposed solutions (Q2).

V. CONCLUSION

The set of technologies that defines an IoT environment is rapidly evolving. The concerns with security are reflected in the articles discussed in this paper and others that did not meet the outlined criteria. The same way, different approaches suggest solutions to different scenarios.

The aim of this work was to map security problems and respective solutions to sensors networks in IoT environments. Four categories of problems and nine solution categories were defined, presenting uneasiness with the lack of confidentiality and suggestion, especially in cryptography.

The superficial analysis in this paper suggests a deeper study to compare effectiveness and application of presented solutions is necessary. It is important to work and understand what makes confidentiality the most exposed problem and explore best applicable approaches. A survey is a great suggestion to continue the research in future papers.

REFERENCES

[1] K. Ashton. "That ‘internet of things’ thing.", RFiD Journal, vol. 22, no.7, 2009, pp. 97-114.

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

[3] B. Burton and M. Walker. "Hype Cycle for Emerging Technologies, 2015.", 2015.

[4] L. Tan and N. Wang. "Future internet: The internet of things." 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), vol. 5. IEEE, 2010, pp. 376-380.

[5] M. Chaqfeh and N. Mohamed, “Challenges in middleware solutions for the internet of things”, In Collaboration Technologies and Systems (CTS), 2012 International Conference on. IEEE, 2012, pp. 21-26.

[6] P. Kumari, M. Kumar, and R. Rishi, “Study of Security in Wireless Sensor Networks” In

Proceedings of International Journal of Computer Science and Technology, vol. 1, no. 5, 2010, pp. 347-354.

[7] K. Petersen, R. Feldt, S. Mujtaba and M. Mattsson, “Systematic mapping studies in software engineering” In Proceedings of the international conference on Evaluation and Assessment in Software Engineering, 2008, pp. 68-77.

[8] B. A. Kitchenham and S. Charters, “Guidelines for performing systematic literature reviews in software engineering”, Technical Report EBSE 2007-001, Keele University and Durham University Joint Report, July 2007. 2.4, 2.4, 3.1, 3.2.1, 3.2.2, 4.1, 5.1, C.2, C.3

[9] L. Atzori, A. Iera, and G. Morabito. “The Internet of Things: a Survey”, Computer Network, vol 54, no. 15, pp. 2787-2805, 2010.

[10] A. Rodrigues. A. Ordóñez, H. Ordóñez, and R. Segovia, “Adapting NSGA-II for Hierarchical Sensor Networks in the IoT” Procedia Computer Science, vol. 61, pp. 355-560, 2010.

[11] K. Främling and M. Maharjan, “Standardized Communication Between Intelligent Products for the IoT” IFAC Proceedings, vol. 46, no. 7, pp. 157-162, 2013.

[12] B. Guo, D. Zhang, Z. Wang, Z. Yu, and X. Zhou, “Opportunistic IoT: Exploring the harmonious interaction between human and the Internet of things”, Journal of Network and Computer Applications, vol 36, no 6, pp. 1531-1539, 2012.

[13] A. Rettig, S. Khanna, and R. Beck “Open source REST services for environmental sensor networking” Applied Geography, vol 60, pp. 294-300, 2014.

[14] V. Rocha, F. Ferraz, H. Souza, and C. Ferraz. “ME-DiTV:A Middleware Extension for Digital TV”, unpublished.

[15] R. Maciel and S. Assis. “Middleware: Uma solução para o desenvolvimento de aplicações distribuídas”. CienteFico, Year IV, vol. 1, 2014.

[16] A. Cavalcanti, C. Albuquerque, and A. Furtado. “A Study on middleware for IoT”, unpublished.

[17] Q. Zhu, R. Wang, Q. Chen, Y. Liu, and W. Qin “IOT Gateway: Bridging Wireless Sensor Networks into Internet of Things” International Conference on Embedded and Ubiquitous Computing on IEEE, 2010, pp. 347-352.

[18] I. Chatzigiannakisa, A. Vitalettia, and A. Pyrgelis “A Privacy-Preserving Smart Parking System based on an IoT Elliptic Curve Based Security Platform” Computer Communications vol. 89-90, pp.165-177, 2010.

[19] N. Ntul and A. Abu-Mahfouz “A Simple Security Architecture for Smart Water Management System” Procedia Computer Science, vol. 83, pp. 1164-1169, 2016

[20] P. Belsis and G. Pantziou “A k-anonymity privacy-preserving approach in wireless medical monitoring environments” Pers Ubiquit Computing, vol. 18.1, pp. 61-74, 2014

[21] P. Gope and T. Hwang “BSN-Care: A Secure IoT-based Modern Healthcare System Using Body Sensor Network” IEEE Sensors Journal, vol. 16, no. 5, pp. 1368-1376, 2016

[22] X. Caron, R. Bosua, S. Maynard, and A. Ahmad “The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective” Computer Law & Security Review, vol. 32, no. 1, pp. 4-15, 2016.

[23] K. Mandal, X. Fan, and G. Gong “Design and Implementation of Warbler Family of Lightweight Pseudorandom Number Generators for Smart Devices” Department of Electrical Engineering, University of Washington, vol. 15, no. 1, 2016

[24] Greenough. “How the 'Internet of Things' will impact consumers, businesses, and governments in 2016 and beyond” Business Insider, 2016.