INTERNET OF THINGS – SECURITY SURVEY

[1] V. Vaneeswari, [2]S. Selvakumari, [3]S.Ranichandra
[1][2][3] Assistant Professor,
Department of Computer Science
Dhanalakshmi Srinivasan College of Arts and Science for Women (Autonomous)
Perambalur.

ABSTRACT

The internet of things (IoT) is a technology that has the capacity to transfigure the way that we live, in sectors ranging from transport to health, from entertainment to our communications with government. This incredible opportunity also presents a number of major challenges. The growth of the number of devices and the pace of that development pose challenges to our security and freedoms as we struggle to develop the policies, standards and governance that shape this development without hindering innovation. This article talks about the development of IoT, its different definitions, and some of its key application areas. Security and privacy reflections and challenges are discussed in general and in the context of these applications.

KEYWORDS:

Internet Of Things, protection, confidentiality, hope.

1. INTRODUCTION

The Internet of Things (IoT) is referred to as a development that can deliver dramatic changes in the way we live. It is recognized as an operator that enhances efficiency in many areas, including transport and logistics, health and manufacturing. IoT will help improve processes through advanced data analysis, and will capitalize on its cyber-physical properties to drive new market segments, leading to cross-cutting applications and services (Miorandi et al. 2012).

THE PROGRESSION OF THE IOT

The idea of connecting 'things' to the Internet stretches far beyond the use of the term 'Internet of Things'. In the early 1980s, Carnegie Melon University students fitted Internet-linked photo sensors into a cool vending machine that allowed them to calculate the number of cans distributed. This helped determine how many drinks were distributed to anyone with Internet access and how many remained (Wetter 1995).

Even before the first webpage was created, John Romkey and Simon Hackett introduced a toaster connected to the Internet in the 1990s. Romkey's presentation at the 1990 Interrope Conference featured the Internet - enabled Sunbeam Deluxe Radiation Control Toaster, which resulted in a challenge to Romki from Dan Lynch, President of Intrope at the previous year's conference. The toaster was connected using TCP / IP and had a simple networking management protocol Management Information Platform (SNMP MIB) controller; One of its functions is to turn the power on or off. The first use of the term 'Internet of Things' came much later, and was widely used in 1999 when Ashton (Ashton 2009) used it as the title of a presentation on Procter & Gamble.

THE DEVELOPMENT OF THE IOT

There has been a rapid growth in the number of devices connected to the Internet. Many analysts, particularly Cisco and Ericsson (Dave Evans and Hans Westburg, respectively), predict that by 2020, 50 billion devices will be connected to the Internet. Of course, these ratings are hard to confirm with confidence, both have now revised their ratings. Ericsson estimates 30 million whistles will be worth $ 28 billion by 2021. One reason why growth is difficult to predict is that today there are not even statistics on the number of devices connected to the Internet. Not only is there a significant difference in the statistics using the same definitions, but the complexity of the different interpretations of the IoT also has an impact. Some figures clearly distinguish between machine-to-machine (M2M) and IoT devices, such as GSMA, M2M's analysis focuses on cellular M2M connectivity and excludes computer devices in consumer electronics such as smartphones and e-readers. , Tablets, as well as other types of

M2M connectivity technologies that support the vast universe of the Internet of Things (IoT) '(KCH 2015

DEFINING THE IOT

When writing about the first use of the word IoT, Ashton noted that the term is ‘often misunderstood’. In fact, today there are many definitions and interpretations of IoT (Atzori, Iera, and Morabito 2010; Bandyopadhyay and Sen 2011; Malina et al. 2016). This can be expected when considering the general public or researchers with a vague interest in the field, but this is most surprising when more specialized researchers vary in definition. For example, IEEE in its special report: IoT (IEEE 2014) describes IoT as ‘a network of items - each embedded with sensors - connected to the Internet’. IoT can be seen to be associated and evolving with various technologies, visions and research directions. Stankovic (2014) recognizes that policies and research questions overlap in five different research communities: IoT, mobile computing, widespread computing, wireless sensor networks, and cyber-physical systems. Adsori, Ira and Morabito (2010) consider IoT to be a combination of three main visions: 'things' oriented (e.g. RFID, NFC, wireless sensor actuators), 'Internet' oriented (a. E.g. IP for smart objects) and 'semantic' based (e.g. rational on data).

Considering its evolution, however, it becomes clear that IoT integrates various key areas, further complicating the problem of defining and differentiating IoT. Considering the close relationship with other visions and developments, and the lack of a general understanding of the definition and scope of IoT, or what 'things' really are, it is not surprising that there are challenges in security, privacy and policy. IoT.

CORRELATION TO M2M AND THE IOT:

M2M communication is a term commonly used today, especially given the debate surrounding the Fourth Industrial Revolution and the Industrial IoT, but it has a much longer history. Basic Marine Management Solutions and Supervisory Control and Data Acquisition (SCADA) solutions have relied on M2M communications for decades (Morish 2014), before the use of M2M communications allowed the use of ATMs and point-of-sale systems.

M2M involves straight communication between devices without human involvement. This communication can be over any channel, wire or wireless, and the number of technologies, standards and protocols for communication is large and growing. Cellular networks (GSM, 3G, 4G), or between devices (without going through a base station, intermediary or access point) can communicate in a point-to-point manner, each with a different surface area. Some of the major communication technologies include WiFi, RFID, Dedicated Short Range Communication (DSRC), Bluetooth, Bluetooth Low Energy (now referred to as Bluetooth Smart), NFC and ZigB. Include.

In this study, we present a discussion of security and privacy challenges in IoT, illustrated by several key applications. This article first presents an overview of the widespread uses of IoT and the various classifications found in the literature. Before outlining the general security and privacy issues in IoT, it outlines several specific areas of application. The impact of IoT on security and privacy concerns is then discussed before final decisions and recommendations are made in areas of major concern.

APPLICATIONS OF THE IOT

IoT is making a significant impact in many fields, and many researchers have provided insights and analysis into its applications. When providing applications for IoT, researchers have their own classification of domains and applications. Each classification has its own merits, and it depends not only on the goal to be achieved, but also on the definition and context of the IoT under consideration.

Application domains are provided by professionals and educators. For example, the industry brochure Liblium (2015) lists 61 applications for IoT across multiple domains using different sensor boards. Educational initiatives include Adsori, Ira and Morabido (2010), which categorize applications into four short- and medium-term types (transportation and logistics; sanitation; Smart environment - home, office, plant; Personal and social) and long-term future type. Miorandi et al. (2012) Authors use six types, while others modify and maintain the health field. Most importantly, however, they do not focus on the personal and social domain, but instead introduce the type of security and surveillance. Whitmore, Agarwal and Sue 2015 use a modified classification based on an updated literary review, most notably in the works of Atsori, Ira, and Morabido (2010) and Miorandi, among others. (2012). This classification is distributed with a temporary future vision and restructures the transport and logistics and smart environment domains,

recognizing IoT's significant role in distribution chains and its relationship with the logistics industry, thus creating a category specifically for distribution chains and logistics. In addition, a new category called Smart Infrastructure is being introduced, which expands Adsori's smart eco-domain and introduces transportation infrastructure features. Janella et al. (2014) focus on the Smart City, while Da Soo, Hee and Li (2014) focus on the industry applications of IoT, and include the consideration of the main case of IoT used for firefighting. The authors of this latter paper extend their work to a wider range of applications (Li, Da Soo, and Zhao 2015), combining it with the ideas of Adsori and Miorandi. Perera et al. (2014) and Pandiopadhyay and Sen (2011) are both very impressed with the report from CERP to IoT (Vermason et al. 2011). This report defines three essential application domains for IoT: industry, environment and community. However, the report found that it is difficult to isolate any of these domains, but rather applications and services at the internal and inter-domain level. Instead, we consider applications (which support one or more of the above domains) and services that meet a specific function or requirement at an internal or inter-domain level. So, if companies want to consider their cyber security risk, doing so at the domain level would be a misconception, albeit obviously intuitive. The fact that there are so many ways to consider domains and applications should tell us that this way of thinking about risk does not help. Domain threat modeling and risk assessment may have similar themes and may have radically different risks. Therefore, rather than considering the cyber security risk at the domain level, we need to explore the many IoT applications between domains. We now discuss a small selection of applications that have significant cyber security risks, indicating the potential for greater impact and / or attack.

2. ASSOCIATED AND INDEPENDENT VEHICLES

The use of sensors in the automotive industry is one of the biggest growth areas (Miola 2016). There are a significant number of sensors within the vehicle used for everything from engine operation to computer monitoring, emission control and brakes. Examples include Bluetooth-enabled tire pressure monitoring systems, crank level, cam level, multiple absolute pressure and throttle level. Sensors are embedded as an integral part of the transport infrastructure, and there are significant investments in the UK, for example, with the introduction of the Highways UK Smart Motorways project (Bull 2012). Other initiatives include developing infrastructure and communications in urban environments. UKCITE (www.ukcite.co.uk) is an affiliate in the UK and funded by the Autonomous Vehicle Center and the innovative UK (part of a $ 100 million investment plan in research and development) that has over 40 miles of weapons on urban roads, twin trucks and Motorways with communication technology. The use of vehicle first infrastructure (V2I) communications allows for better traffic flow, especially in urban and suburban environments (Fajipur et al. 2012). Communication between vehicles, also known as V2V communication, through technologies such as DSRC, Long Evolution for Vehicles, and Visible Light Communications, enables cars to reduce energy consumption and provide early warning of events. Deployment of such intelligent transport systems using Edge and Cloud technology may assist in accident management, location-based traffic and weather notifications, thereby supporting assisted driving (Atsori, ERA and Morabido 2010).

BUILDINGS, HOMES, AND OFFICES

Demand for smart home devices has grown significantly, with 161 million units shipped between 2010 and 2016, according to the IHS Market (IHS 2016); More than half of these devices were delivered in 2016, an increase of 64 percent over the previous year. The increase included the acquisition of smart energy management systems such as Nest thermostats, security solutions such as August smart locks and personal home assistants such as Google Home, Poshin Mickey and Amazon's Alexa.

RETAIL

With the increased benefits of sensor technologies, IoT has the potential to enhance the consumer experience in retail stores and businesses. Monitoring and controlling the performance of operational data and equipment, for example, will allow businesses to improve performance by monitoring progress in real time (Lee and Lee 2015). Sensors generate large amounts of data over time, which can be used to determine potential vulnerabilities and to embrace businesses through big data and business analysis. Understanding customers' market trends and demands through advanced market analysis can lead to reactive and efficient delivery, which can control resource wastage and growth, which ultimately fail to detect demand. With the greater acceptance of IoT, retailers can not only ensure appropriate purchases and deliveries, but also offer customers different products

that best suit their needs. For example, a user may purchase certain consumer electronics devices, but alternatively there may be products that provide adequate levels of operation, battery life, and so on. This result can be gleaned from the information collected from the sensors and, as we choose to update our mobile phone or internet packages, we can seek advice from suppliers on the service that best suits our needs. Customer satisfaction can also be achieved through integrated retail, as well as customer recognition and environmental awareness offers (McCauley, Bucklew and Chung 2015).

CULTIVATION

Smart technology is also being developed in the field of agriculture. Domain information is traditionally obtained through manual reporting methods, which can lead to errors in the data. Properly increasing the efficiency and reducing the manual labor can contribute to the scientific cultivation with increased quality of IoT sensors and technologies to increase and regulate the production of agricultural products (Chen and Jin 2012). It is implemented by monitoring environmental parameters such as air pressure, humidity and wind direction through wireless sensors, which help in cultivation by adapting to agricultural needs. The Elliott Review (Elliott 2014) highlighted the importance of food discovery. IoT can play a significant role in improving warranty, logistics and supply chain management through surveillance and tracking systems.

3. SECURITY CHALLENGES WITHIN THE IOT

As IoT expands and becomes more and more intertwined with the fabric of our daily lives and becomes increasingly an integral part of our vital national infrastructure, it is vital to safeguard its systems. CIA Information Security (Confidentiality, Integrity and Availability) The first five pillars of information security (confidentiality, integrity, availability, reliability and non-negotiation) and the protection of systems based on multiple principles. Parkerian Hexod (Confidentiality, Integrity, Availability, Credibility, Possession and Use) (Parker 1998). Research articles discussing security concepts related to cyber-physical (contrary to information) and IoT systems differ in what policies they follow. The majority of researchers believe that the CIA Barkarian Hexat, originally offered as an improvement over the CIA's limitations, is often rejected; In fact, the use of hexat has been the subject of debate among security experts (Ferruza and Kim 2007). However, it must be recognized that this is not an exhaustive list of security challenges.

4. PHYSICAL BOUNDARIES OF DEVICES AND INTERACTIONS

In any application area, IoT devices are usually fixed with low-power and low-part processors, and are standard as ‘Internet Protocol can be applied to smaller devices’ (Mulligan 2007). Barriers on IoT devices limit the ability to process information quickly - with limited CPU, memory and energy budget. This means challenging security models are needed that meet the competitive goals of robust performance and minimal resource consumption. Barriers to size and power impact are very significant in efforts to maintain confidentiality and integrity in IoT systems.

5. AUTHENTICATION AND IDENTITY MANAGEMENT

Identity management is about the unique identity of objects, and authentication then confirms the identity relationship between the two parties (Mahale et al. 2010). The CERP report (Vermason et al. 2011) recognizes the need for further research on the ‘development, integration and dynamics of technologies for global identifiable identification and recognition’.

Authentication within the IoT is important because without proper authentication confidentiality, integrity and availability of systems can be compromised. This is because, if an adversary can be recognized as a legitimate user, they can access any data held by the user and see (compromising confidentiality), Modifying (compromising integrity), and eliminating or restricting as much as possible available to the user (compromising availability).

Recognizing and identifying users in IoT is a significant challenge. Currently, username / password pairs are the most common form of identifying and identifying users in electronic systems, although other formats such as shared keys, digital certificates, or biometric credentials may be used (Kessner et al. 2012). However, IoT's ubiquitous view will eliminate many of the physical communication interfaces to which usernames and passwords are sent.

6. IMPLEMENTATION, UPDATING, RESPONSIBILITY, AND ACCOUNTABILITY

Implementing and updating security should be manageable and cost effective, although this is often overlooked in the debate. IoT systems can be geographically remote and include sensors and actuators in extreme and challenging environments. To protect the computer's cyber security, it is essential that any vulnerabilities are detected as soon as they are detected. Therefore, remote access is required to allow these system updates. The latest software connections can be installed dynamically, and this process is managed by the Cloud Assistance Framework; However, designing a secure mechanism for dynamic installation is a challenging task (McLarese et al. 2016). It should also be acknowledged that updates may change the functionality of devices, and these changes do not always match user expectations (Rose, Eldridge and Sobin 2015). For this reason, if a user has a responsibility or control over the use of a link, they may decide to resist updating if they feel the risk of compromise outweighs the negative impact of the process (Cavusoglu, Cavusoglu and Zhang 2008). The Tyne attack in 2016 illustrates the significant impact of the botnet service's refusal to distribute attacks on unattended printers, IP cameras, residential gateways and child monitors. This guides to another important challenge regarding answerability, responsibility and accountability in IoT. Determining liability and liability is a challenge as IoT has different devices, communications, infrastructure and services under different control and ownership. When legal liability is with one company, the impact of a harmless attack on one component can cause catastrophic, irreversible damage to another company.

7. SECURITY ISSUES IN CONNECTED AND AUTONOMOUS VEHICLES

The Connected and Autonomous Vehicles (CAV) area is complex and includes a wide variety of sensors, actuators, infrastructure, communication protocols and services. These services vary from small, simple services that operate on only a few components, to global services that cover significant areas of vital national infrastructure. This work cannot cover all types of system and potential and executed attacks. However, it is possible to highlight some of the most important attacks.

Modern vehicles have 70 to 100 integrated electronic control units (ECUs) for applications such as braking, steering, transmission, suspension and engine control. The sensors that provide information in these ECUs include the tire pressure monitoring system infotainment system, camera, lidar, radar and brake and engine sensors. Communicate with ECUs through network types including CAN (Controller Area Networks), Flexray, MIA (Media Oriented System Transport) and LIN (Local Internet Connect Network). Different manufacturers use different networks, but modern vehicles have many of these network types. However, these protocols are designed to prioritize performance and safety over safety. Chekhov et al. (2011) and Kosher et al. Miller and Wallace's work was highly publicized in 2015, in which they used remote execution to inflict damage on Jeep Cherokee (Mansfield-Devin 2016). They were able to control the vehicle while it was in motion.

8. PRIVACY CHALLENGES IN THE IOT

IoT (Misra, Maheswaran, and Hashmi 2016; Zikari et al. 2015; Ziegildorf, Morsen & Wehrley 2014; Roman, Nazra and Lopez 2011; Kessner et al. 2012) see privacy as a major concern. IoT provides data owned not only by consumers such as the World Wide Web, but also by citizens, groups and organizations in general. It can be used to establish what we want, where we are going, and our intentions. While this can provide better opportunities for advanced services, it should be weighed against our desire for privacy. It is important for consumers to trust the services they engage in to respect their privacy. Confidence is a fundamental element in the formation of any relationship, and it is a key factor in the adoption of new technology (Yan, Zhang and Vasilkos 2014). People will not use new technology if they do not have enough confidence in protecting privacy, security and safety (Dadio and Flority 2011; IBM Watson Foundation 2015), which is especially true in complex systems such as IoT.

Sensors collect various data about the lives of citizens, including those embedded in mobile devices. This data will be consolidated, analyzed, processed, linked, and truncated to obtain useful information to enable intelligent and ubiquitous services. The Foundation refers to determining when, to whom or to whom information should be published (Yann and Holdmans 2008).

Various privacy development technologies have been developed to ensure privacy, including virtual private

networks, traffic layer security, DNS security extension, onion route and private information retrieval (Weber 2010).

Privacy Policy Languages are another type of PET, and Privacy policy languages are another type of PET, and the previously discussed P3P program may be considered to belong to the PET class of PPLs (Wang and Kopsa 2009). PPLs can be classified as external (declaration without enforcement) or internal (protocol with support for enforcement); B3B falls in the former class. The previously discussed P3B project may be considered to belong to the PED class of PPLs (Wang and Kopsa 2009). PPLs can be classified as external (declaration without enforcement) or internal (protocol with support for enforcement); B3B falls in the former class. Other PPLs include SAML (Security Confirmation Markup Language), XACML (an oasis standard for access control), and PPL, A-PPL, and GeoXAML are XACML extensions; XACL; SecPAL and its extension to refer to the handling of personally identifiable information, SecPAL4P; AIR (Accountability in RDF); Express; P2U; EPAL; P-RPAC; Flex.ddpl; Jeeves; BS Long; Conspec; And slang (see Casem-Madani and Meyer 2015 and Haynes et al. 2016 for more information). While there is a limit to PPLs, nothing comes out as a real standard, and large-scale adoption remains a challenge.

9. CONCLUSIONS AND FURTHER WORK

In this article we discussed the origin of IoT and how it can be a major challenge to standardization and overall vision. This has led to challenges to security and warranty in IoT.

Promoting standardization and integration in IoT is the most important challenge, but also the most fundamental. In terms of process and technology it is not only difficult, but also political. All stakeholders should be considered and have their conflicting opinions about IoT. The B3B project highlights the difficulties in gaining consensus and trust between parties with different visions and interests.

The B3B project was commendable, but faced considerable difficulties. A similar system for IoT would certainly benefit, but it is challenging to ensure that its results are relevant and acceptable to all. If there is to be a protocol similar to P3P, it is important to learn lessons from P3P to communicate how data is captured, processed, stored and transferred, and to provide users with a way to have control over their data selection and control. For any standard to be successful, it is important to consider the politics involved in this project. Privacy advocates may see this development as an industrial maneuver, a critique equated to the P3B plan; The protocol should not allow services to create the illusion of privacy when collecting personal data. It must be recognized that any quality can only be part of a solution, and that implementing quality alone does not provide adequate protection. It is therefore recommended to use the standard in conjunction with other privacy enhancement tools. Any standards must be developed in accordance with legal and regulatory compliance. If there is no compliance or financial implication for non-implementation of the protocol, the business case for the protocol will fail. To increase the likelihood of industry adoption and user acceptance, there should be no protocol for managing consent in IoT:

- Mission was built around concrete agreements to ensure that there were no mission creeps and that the objectives were clear;
- Simple, economically efficient and operational;
- Note any impact on current and future business models;
- Body created in association with industry organizations (service and infrastructure providers) and user representative groups;
- Developed in accordance with Legal Legal and Regulatory Compliance. Without compliance or financial implication for non-implementation of the protocol, the business case for the protocol will fail.

10. REFERENCES

1. ABI Research. 2017. “What Is the Internet of Things?” Accessed July 4, 2017. https://www.abiresearch.com/pages/what-is-internet-things/. [Google Scholar]

2. Abomhara, Mohamed, and Geir M. Køien. 2014. “Security and Privacy in the Internet of Things: Current Status and Open Issues.” International Conference on Privacy and Security in Mobile Systems (PRISMS), Aalborg, Denmark, May 11–14, 1–8. [Google Scholar]

3. Al-Fuqaha, Ala, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. 2015.

"Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications." *IEEE Communications Surveys & Tutorials* 17 (4): 2347–2376. [Crossref], [Web of Science ®], [Google Scholar]

4. Ashton, Kevin. 2009. "That "Internet of Things" Thing." *RFiD Journal*, 97–114. [Google Scholar]

5. Atzori, Luigi, Antonio Iera, and Giacomo Morabito. 2010. "The Internet of Things: A Survey." *Computer Networks* 54 (15): 2787–2805. doi:10.1016/j.comnet.2010.05.010. [Crossref], [Web of Science ®], [Google Scholar]

6. Balduzzi, Marco, Alessandro Pasta, and Kyle Wilhoit. 2014. "A Security Evaluation of AIS Automated Identification System." Proceedings of the 30th Annual Computer Security Applications Conference, New Orleans, LA, December 8–12, 436–445. [Google Scholar]

7. Bandyopadhyay, Debasis, and Jaydip Sen. 2011. "Internet of Things: Applications and Challenges in Technology and Standardization." *Wireless Personal Communications* 58 (1): 49–69. doi:10.1007/s11277-011-0288-5. [Crossref], [Web of Science ®], [Google Scholar]

8. Barnes, Susan B. 2006. "A Privacy Paradox: Social Networking in the United States." *First Monday* 11 (9). doi:10.5210/fm.v11i9.1394. [Crossref], [Google Scholar]

9. Beatty, Patricia, Ian Reay, Scott Dick, and James Miller. 2007. "P3P Adoption on e-Commerce Web Sites: A Survey and Analysis." *IEEE Internet Computing* 11 (2): 65–71. [Crossref], [Web of Science ®], [Google Scholar]

10. BITAG. 2016. "Internet of Things (IoT) Security and Privacy Recommendations." BITAG Broadband Internet Technical Advisory Group, November 2016. http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf. [Google Scholar]

11. Blank, Grant, Gillian Bolsover, and Elizabeth Dubois. 2014. "A New Privacy Paradox: Young People and Privacy on Social Network Sites." American Sociological Association Annual Meeting, San Francisco, CA. Accessed July 4, 2017. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2479938. [Google Scholar]

12. Bojanova, Irena, George Hurlburt, and Jeffrey Voas. 2014. "Imagineering an Internet of Anything." *Computer* 47 (6): 72–77. doi:10.1109/MC.2014.150. [Crossref], [Web of Science ®], [Google Scholar]

13. British Land. 2017. "Smart Offices | British Land – The Office Agenda." Accessed July 4, 2017. http://officeagenda.britishland.com/smart-offices. [Google Scholar]

14. Bui, Nicola, and Michele Zorzi. 2011. "Health Care Applications: A Solution Based on the Internet of Things." Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies, Barcelona, Spain, October 26–29, 1–5. ACM. [Google Scholar]

15. Buxmann, Peter, Thomas Hess, and Rainer Ruggaber. 2011. "Internet of Services." *Business & Information Systems Engineering* 1 (5): 341–342. [Crossref], [Web of Science ®], [Google Scholar]

16. Cavalry. 2014. "Five Star Automotive Cyber Safety Framework." I Am The Cavalry, August 2014. Accessed July 4, 2017. https://iamthecavalry.org/5star. [Google Scholar]

17. Cavalry. 2016. "Hippocratic Oath for Connected Medical Devices." I Am The Cavalry, January 2016. Accessed July 4, 2017. https://iamthecavalry.org/oath. [Google Scholar]

18. Cavusoglu, Hasan, Huseyin Cavusoglu, and Jun Zhang. 2008. "Security Patch Management: Share the Burden or Share the Damage?." *Management Science* 54 (4): 657–670. [Crossref], [Web of Science ®], [Google Scholar]

19. Cerf, Vinton G. 2015. "Access Control and the Internet of Things." *IEEE Internet Computing 19* (5): 96–c3. doi:10.1109/MIC.2015.108. [Crossref], [Google Scholar]

20. Cha, Inhyok, Yogendra Shah, Andreas U. Schmidt, Andreas Leicher, and Michael Victor Meyerstein. 2009. "Trust in M2M Communication." *IEEE Vehicular Technology Magazine* 4 (3): 69–75. [Crossref], [Web of Science ®], [Google Scholar]