THE IMPACT OF SECURITY AND DATA PRIVACY IN THE INTERNET OF THINGS APPLICATIONS

Roxana HUCANU IBANESCU
Alexandru Ioan Cuza University of Iaşi, Faculty of Economics and Business Administration
Iaşi, Romania
roxana_hucanu@yahoo.com

Abstract*: In recent years, the world of networks has been marked by the emergence of a new technology called the Internet of Things, which aims to create new values through the exchange of information and knowledge between people and objects. This technology is different from its predecessors (Traditional Internet, Mobile Internet, Sensor Network, etc.), focusing in particular on ubiquitous service models, heterogeneous network architectures and universal access for people, things, objects and processes. Innovations and future research on IoT applications and services are driven by the high potential for market and profit. However, IoT proposes new areas to study vulnerability in system security and more difficult confidentiality issues. Today's industry and government organizations underline cybersecurity and privacy as top IT priorities. Online threats are presented by both individuals and groups organized with the intent to commit commercial theft, disturbance actions and invasion of systems for activist and espionage purposes.*
Keywords*: Internet of Things, security, data privacy*

1. INTRODUCTION

Internet of Things (abv. IoT) represents a useful and fascinating world where physical devices used in our everyday life are connected to the Internet. Within the Internet of Things sensors and communications devices are integrated into physical objects for facilitating the communication between objects or between objects and other devices like cloud servers, computers, smartphones, tablets. According to the Cisco Internet Business Solutions Group (IBSG), IoT represents that period of time where more "objects" were connected to the Internet than people (Evans, 2011).

The term "Internet of Things" was first used by Kevin Ashton in 1999 at MITi to illustrate the connecting power of RFIDii tags, used in supply chains, to the Internet in order to control stocks of goods without the need for human intervention (Ashton, 2009). In the current context, the Internet of Things refers to the devices that have an advanced degree of connectivity to systems and services that interact with each other and cover a wide range of protocols, areas and applications. We can bring into discussion a large number of applicability areas, including energy, transport, buildings, house, health, cities, sales, agriculture and others. We can think about of an autonomous home future. He will automatically start the TV on a favorite channel or ambient music when the owner's smartphone has left the car or walks in the door of the house. He will be connected to the Internet all the time and communicate with the automated home system. It can also initiate some certain protocols, such as opening doors and lighting bulbs. Or we can use a fitness bracelet to measure heart rate and temperature and then communicate with the automated home system to create a perfect room temperature depending on the obtained

information. The collected information can be shared with different stakeholders and used to improve business intelligence.

Thanks to this technology our life is improved a lot and makes it easier for us to carry out everyday tasks. But it also comes with less good parts, including the invisibility of the data collection. The privacy of Internet of Things users could easily be sacrificed (Fink, et al., 2015). When we use the application/service automatically we expect from the service providers to deliver tailored services based on collected information from our used application, protect our information from unauthorized access and not share those data with 3rd parties (Sun, et al., 2014). The existence and use of IoT applications creates challenges for the security of the entire IoT ecosystem, from reasons related to the extension of the "Internet" through the traditional network (Internet, cellular data network, sensor network), the network connection of the objects due to the fact that every object will be connected to the Internet, the communication between objects. Gartner placed security at the top of its list of top 10 IoT technologies for 2017 and 2018, saying "IoT security will be complicated by the fact that many 'things' use simple processors and operating systems that may not support sophisticated security approaches" (David, 2016). We should pay more attention to the research issues for confidentiality, authenticity, and integrity of data in the IOT.

2. SECURITY AND PRIVACY CONSIDERATIONS

As we rely on connected devices to make our lives better and easier, we need to take in fact a very important aspect, namely security. Security is defined as a set of mechanisms used to protect sensitive data from cyberattacks and to guarantee the confidentiality, integrity, and authenticity of data. All the participants from the IoT ecosystem must take the responsibility for the security of the data, devices and offered services by implementing and respecting the best practices (Sarah, 2017).

2.1. Security Architecture

Before going to the discussion about the impact of security in IoT systems, we must first understand and analyze the IoT security architecture. The architecture is divided into four layers, including the application layer, support layer, network layer, and perception layer (see Figure 1). In some systems, the processing layer is represented by the network support technologies, such as middleware, computing, network processing (Zhao & Ge, 2013).

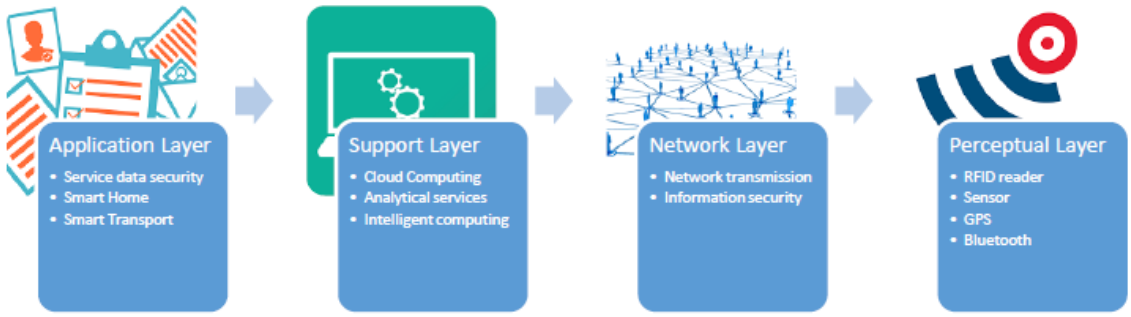

Figure 1 IoT Security Architecture

IoT must ensure the security of all layers. In order to analyze and describe the security issues of IoT, according to the data transmission in the Internet of things we will start to describe the architecture from the lowest level, perceptual layer.

A. Perceptual layer

All the information from the physical world is collected through the Perceptual layer using physical devices that have integrated sensors, RFID tags, GPS and other equipment. The collected data contains information regarding object properties, environmental conditions, and others. Sensors represent the key factor in this layer, used to capture data and transform the physical world into a digital world.

 Security features: The perceptual layers are very simple with small storage capacity and they have a small power related to computer. For this reason, on the one hand, it is very hard to create a security system and set up security protection, on the other hand, issues regarding the communications and the impossibility to apply a public key encryption algorithm appear. Data obtained from sensors need protection for integrity, authenticity, and confidentiality.

 Security requirements: At this node, the authentication is used to ensure the confidentiality of information transmission between layers and to prevent illegal layer access. In this way, the encryption process of data becomes necessary.

B. *Network layer*

Initial processing of information taken from the perceptual layer is made on the network layer along with reliable transmission of information, classification of information and polymerization. The information transmission relies on this layer on several basic networks that are essential for the information exchange that is made between devices, networks as the internet, wireless, satellites, mobile communication, network infrastructure and communication protocols.

 Security features: The protection security mechanism at this layer is very important for the Internet of Things. Even if the core network is relatively safe, attacks like Man-In-the-Middle, counterfeit, junk mail and computer virus still causes damages and cannot be ignored, because a large number of data sending cause congestion.

 Security requirements: Mechanisms for identity authentication (to prevent illegal nodes), data confidentiality and integrality are used to ensure security at this node. A particular attack that is very severe for the IoT and represents a problem that must be resolved in this layer is the distributed denial of service (DDoS).

C. Support layer

After the information passed through the network layer, will be taken over by the support layer whose purpose is to offer a wide range of intelligent computing powers, organizing them using network grid and cloud computing and to create a reliable platform to support the application layer. It plays the role of combining application layer upward and network layer downward. The application layer is the topmost and terminal level.

 Security features: The recognize of malicious information represent a challenge for this layer, due to fact that the support layer is working with mass data processing and intelligent decisions.

 Security requirements: This layer need to work with a variety of application security architecture such as cloud computing and secure multiparty computation, almost all of the strong encryption algorithm and encryption protocol, stronger system security technology, and anti-virus.

D. Application layer

The fourth layer is application layer. According to the needs of the users, that can access the IoT at this point by using the TV, personal computer, laptop, tablet or mobile device this layer deliver personalized services (Ding, et al., 2011).

 Security features: Security needs can be different depending on the environment application and because of the fact that data sharing represents the main characteristic of this layer, it may appear issues related to confidentiality, access control, and information disclosure (Geng, et al., 2010).

 Security requirements: The security problem from application layer can be solved by protecting the user's privacy, using authentication and key agreement. Also, the management of all the password and device should be done in a proper way.

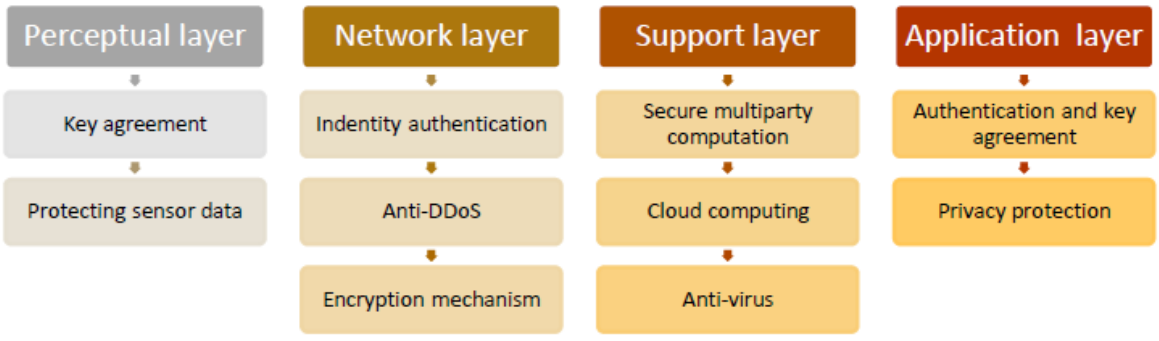

Figure 2 Security requirements for security architecture

2.2. Security services

Therefore, in the security architecture of the process of information transmission, all due consideration must be given to the guarantee of confidentiality, integrity, privacy, authenticity and instantaneity of data and information, which mainly refers to the security of telecommunication network and corresponds to the security of transmission hierarchy in the IoT (Li, 2012).

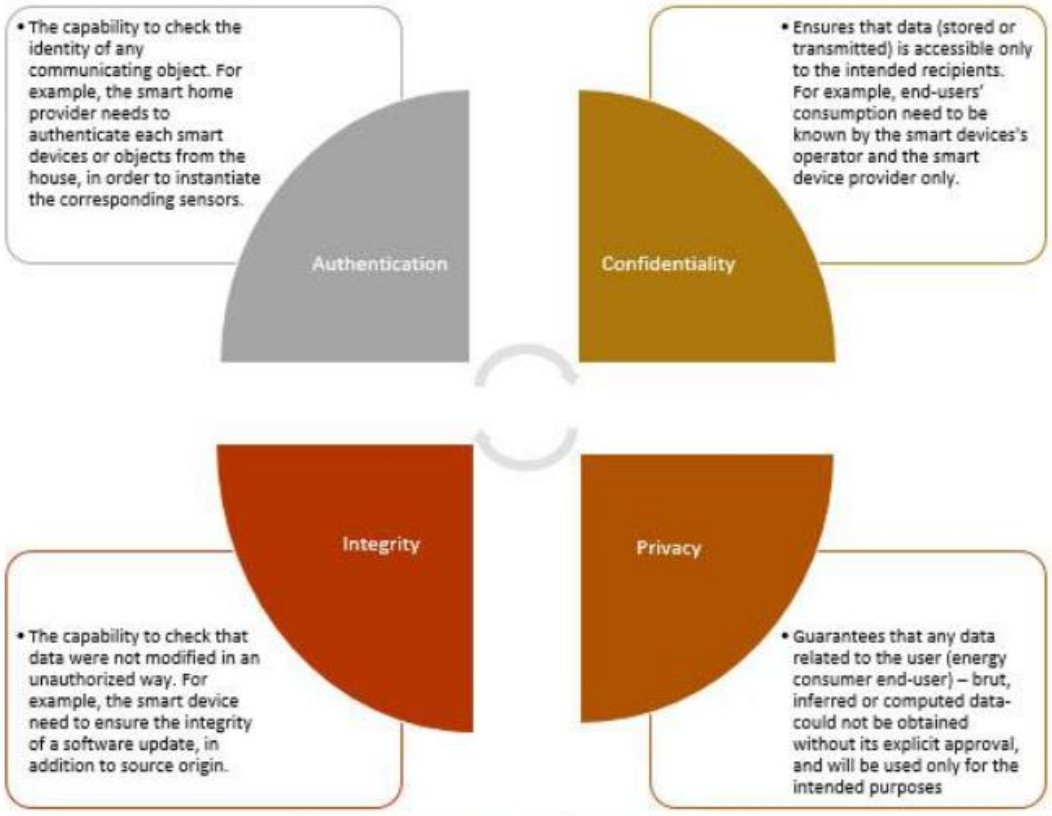

Figure 3 Security services for the IoT

In the presented context, the confidentiality represent a set of rules that limits the access to information, integrity been assured of the fact that the data are accurate and reliable, privacy been the guarantee that users are taking in account their sensitive data and authentication is the guarantee for reliable access to information by the authorized persons. Of all the requirements described above, I believe that confidentiality it should take precedence over the other services as it is a means of protecting information that is carried out by any means between two parties.

2.3 Privacy challenges

Some of the IoT devices are developed in order to create, collect or share data. Therefore, those data cannot be considered "personal data" and they have no impact on confidentiality or consumer's privacy, unrelated to data protection and privacy laws. For example, data refers to

physical state of the machines, metrics regarding the state of network or internal diagnostic (Victor , 2017). The majority of the Internet of Things services involves the creation, distribution and use of personal data about or related to individual consumers and can have impact on consumer's privacy, being related to general data protection and privacy laws. For example, create analysis regarding the individual's state of health or consumer profile based on their shopping habits and favorite supermarkets.

All the stakeholders from the IoT ecosystem have an obligation to respect individuals' privacy and keep personally identifiable or privacy-invasive information secure. A major challenge for the Internet of Things providers is caused by the multiple and often inconsistent laws related to privacy and data protection, laws that can be applied different depending on industry sector, services and implied data types in different countries. For example, a smart vehicle that travels in different countries, therefore the associated data transfers may be governed by each country that the car passes, using different legal jurisdictions. The data obtained from the sensors available in the car, that are used to track the location of the can be used to infer a number of insights about the frequent and favorite places, the driver's lifestyle or hobbies, that can be considered as private information about the user. Also, these insights obtained through 'on-board diagnostics' sensors might be shared with insurance companies who might use those information to impose a higher premium and therefore discriminate against the driver without their knowledge.

Another challenge is represented by the fact that the most data protection laws require companies collecting consumers' data to get the affected consumer's (also known as the 'data subject') consent before processing certain categories of 'personal data' – such as health related data. Most laws are defining the 'personal data' as being any information that relates to an 'identified' or 'identifiable' living, natural person (Gib, 2017). Since, we observe that more and more devices are connected to the Internet and the number of devices is growing (Rob, 2017), the more and more data about individuals will be collected and analyzed and possibly impact their privacy, without necessarily being considered 'personal' by law. It can be obtained detailed user profiles by combining the massive data volumes, big data, cloud storage and predictive analytics.

3. ANALYZING THE SECURITY REQUIREMENTS OF MEDICAL APPLICATIONS

In this example, we study an end-point device, a Wearable Heart Rate Monitor that's a simple device used to measure and record the user's heart rate, in order to provide some indications for better device securing. The device was developed with the intent that the end user will track their pulse data throughout the day, storing it in both the application and the back-end database. The intention is to allow users to review their heart rate over time to track their overall health. Users can watch their health improve or worsen over time, depending on whether they are maintaining a healthy life style. This allows the users to incentivize themselves by evaluating both positive and negative trends in their WHRM data. Data can also be used by partners in order to use these metrics to identify whether a consumer is more or less likely to have a health-related event, such as a heart attack or a stroke.

3.1 Device overview – Wearable Heart Rate Monitor

Figure 4 illustrates a simple hardware design of the Wearable Heart Rate Monitor (WHRM) and its basic components (Mark, 2017).

Figure 4 Wearable Heart Rate Monitor (WHRM)

The Heart Rate Monitor device is composed of standard components for a simple wireless device:

- A Bluetooth Low Energy (BLE) transceiver - provide essentially drop-in wireless connectivity;
- Microcontroller (MCU) enabled for BLE - analyses the data emitted from the sensor and chooses what data should be sent over the BLE transceiver;
- An ambient light photo sensor - used to capture pulse rate data.

In this example, we use a coin cell battery to facilitate the transmission of data between devices, from WHRM to tablet, laptop, or smartphone.

3.2 Service overview

From a service perspective, the application available on the smartphone, laptop or tablet to push metrics from the endpoint up to a back-end service over any available network connection. The back-end service for the application simply associates the device owner with the metrics being captured and stores them in a database local to the application server. The data can be visualized using the mobile application or by using a browser to go on the service's website. On the service provider's websites the users can view and use the captured metrics to perform more actions.

This is a very simple and common service model with no custom or unnecessary complexities (Figure 5).

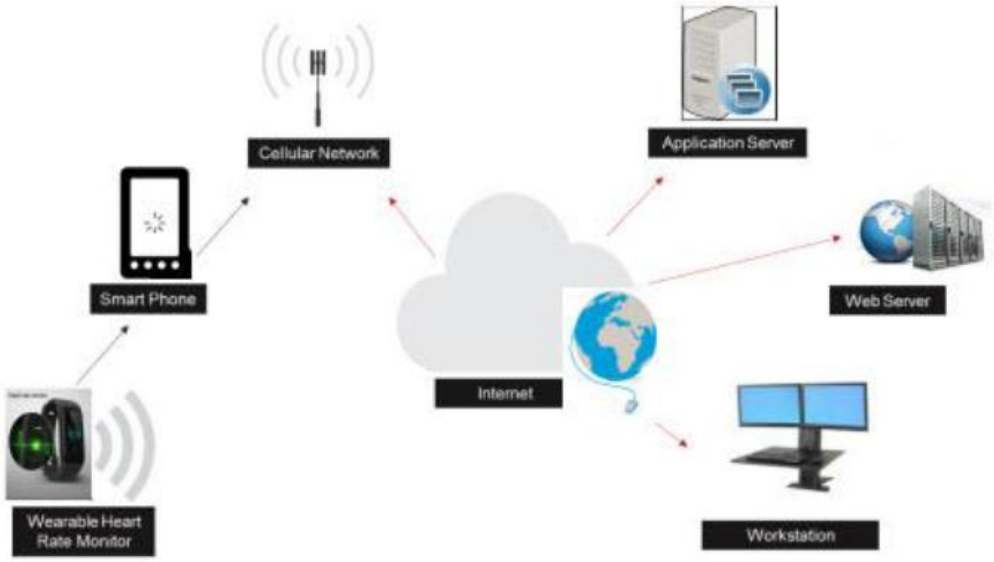

Figure 5 Back-end Service Data Flow

3.3 Security Model

As I see, the most relevant issues that may appear to the product and service can be observe from both perspectives, service and product.

From a product perspective, the issues are related to:

- Cloning;
- Product impersonation;
- Service impersonation;
- Ensuring privacy.

From a service perspective, the issues are related to:

- Cloning;
- Hacked services;
- Identifying anomalous endpoint behavior;
- Limiting compromise;
- Reducing data loss;

- Reducing exploitation;
- Managing user privacy;
- Improving availability.

Considering the fact that the end-point has very little functionality, we can deploy minimal security on the endpoint for both application security and communication. Since the endpoint application is flashed on a single device, as long as the device firmware is locked, there is no real threat of attack against the endpoint within the given use case. Since privacy represent an issue, we must consider at least a personalized PSK version of a Trusted Computing Base (TCB)iii. This would ensure that encryption tokens were unique to each endpoint, so that one compromised endpoint cannot compromise all endpoints. If the personalized (unique) keys were encoded into the locked microcontroller, it would be reasonable to believe that this use case were adequately secured from the threat of cloning, impersonation, and privacy issues.

From a server infrastructure perspective, the things are different because we need to ensure that:

- There must be a front-end security that diminishing the effects of an Denial of Service attack;
- Must be exercised controls to limit the traffic to or from services;
- Duties from the service layers must be well delimited;
- Create secured database with Personalized PSK tokens;
- Define security measures in the service operating system;
- Define the metrics to evaluate anomalous endpoint behavior.

The system can be more secured if we take in account the exposed considerations, and may bring some simple and cost-effective changes on endpoint, ensuring the technology without changing the architecture. Privacy is ensured by granting each endpoint unique cryptographic tokens.

4. CONCLUSIONS

In order to benefit from the huge potential of connected IoT devices, the need for a strict and reliable approach to security is essential. Internet of Things is the next step towards a globally and pervasive connection to any communication and computation enabled objects/devices, regardless their access technology, available resources and location. Security is the main concern for the IoT along with the data privacy because the implementation of IoT on a global scale affects billions of people and devices. In this paper, we briefly reviewed the main security issues and challenges for the Internet of Things and I also described a smart device in order to provide some indications about securing an end-point device.

References

1. Ashton, K., 2009. *That 'Internet of Things' Thing.* [Online] Available at: http://www.rfidjournal.com/articles/view?4986 [Accessed 30 08 2017].
2. David, O., 2016. *Gartner Identifies the Top 10 Internet of Things Technologies for 2017 and 2018.* [Online] Available at: https://www.iotcentral.io/blog/gartner-identifies-the-top-10-internet-of-things-technologies-for

3. Ding, C., Yang, L. & Wu, M., 2011. Security architecture and key technologies for IoT/CPS. *ZTE Technology Journal*, 17(1).
4. Evans, D., 2011. *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, s.l.: Cisco Internet Business Solutions Group (IBSG).
5. Fink, G. A., Zarzhitsky, D. V., Carroll, T. E. & Farquhar, E. D., 2015. Securityand privacy grand challenges for the internet of things. In CollaborationTechnologies and Systems (CTS). *International Conference on*, p. 27–34.
6. Geng, Y. et al., 2010. Security Characteristic and Technology in the Internet of Things. *Journal of Nanjing University of Posts and Telecommunications (Natural Science)*, 30(4).
7. Gib, S., 2017. *Upcoming IoT regulations and laws: How to survive and stay compliant.* [Online] Available at: http://www.ioti.com/security/upcoming-iot-regulations-and-laws-how-survive-and-stay-compliant [Accessed 20 10 2017].
8. Li, L., 2012. Study on security architecture in the Internet of Things.. *Measurement, Information and Control (MIC), 2012 International Conference on*, Volume 1, pp. 374-377.
9. Mark, V., 2017. *Wearables Technology Components.* [Online] Available at: https://www.digikey.com/en/product-highlight/p/panasonic/wearable-technology [Accessed 15 10 2017].
10. Rob, E., 2017. *8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016.* [Online] Available at: https://www.gartner.com/newsroom/id/3598917 [Accessed 02 09 2017].
11. Sarah, K., 2017. *9 IoT Security Threats To Watch.* [Online] Available at: http://www.crn.com/slide-shows/internet-of-things/300089496/black-hat-2017-9-iot-security-threats-to-watch.htm/pgno/0/2 [Accessed 30 09 2017].
12. Sun, G., Huang, S., Yang, Y. & Wang, Z., 2014. A privacy protection policy combined with privacy homomorphism in the Internet of Things. *Computer Communication and Networks (ICCCN), 2014 23rd International Conference on*, 4-7 08, pp. 1-6.
13. Victor , T., 2017. *Internet of Things future forecasts: focus on IoT security.* [Online] Available at: https://www.i-scoop.eu/internet-of-things-guide/iot-security-forecasts/ [Accessed 10 10 2017].
14. Zhao, K. & Ge, L., 2013. A survey on the internet of things security. *Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013*, 14 12, pp. 663-667.