Stand to Research the Privacy Limitations of the Internet of Things in the DID's Perspective

© Mikhail Shpak
Bauman Moscow State Technical University,
Moscow, Russia
Shpak.mike@gmail.com

Abstract. Accelerated growth of the Internet of Things (IoT) expands the implementation of it in our everyday life. The IoT connects artificial intelligence and different physical applications or devices, in order to expand the usage scope and make cities more innovative. A great amount of data produced by the IoT is an example of Data Intensive Domains (DID). The first two parts of this article is a background overview of the IoT and areas, where the IoT is developing. The third part describes the privacy limitations and possible solutions. The fourth part is about the level of IoT privacy limitations in the era of DID. In Conclusion the Research Stand was developed and aims that are planned to achieve.

Keywords: Internet of Things, security, privacy issues, IoT industries, surveillance.

1 Introduction

The Internet of Things is a new era of communication between the people and the devices. Everyone is surrounded with all possible types of electronics, which make life easier. The Internet of Things is a network of smart devices. Smart devices are machines or appliances that utilize different protocols, such as RFID (Radio Frequency Identification), Bluetooth or TCP/IP (Transmission control Protocol) and technics to transfer information over the Internet and exchange the data between the customers and services in the cloud, as described by [1]. The amount of smart devices has already outnumbered the number of employees working in offices, and this number is predicted to grow up-to 26 billion by 2020. Following are some examples of industries, where smart devices are frequently used and how do they produce data.

2 Smart devices as Big Data Producers

Different areas of usage include smart homes, transport and logistics, health and retail industries. We shall consider these devices from the point of possible personal data theft.

Smart home devices are used to smart control door locks, windows, air conditioner, heater, electricity plugs, coffee machines, dishwashers, alarm clock, fire alarm, smoke detectors and window shades. Smart home management is divided into three parts: smart control, smart power-saving and smart application.

Transport industries smart devices are used to provide mobile services in the car with high speed Internet. This feature will enable real time traffic control, interaction with the car manufacturer service for remote diagnostics and improved company logistics automation. Moreover, in the beginning of the self-driven car era, they start to use Internet for information exchange between the cars for better route selection and accident reports.

In health industry smart devices are used by a lot of people. These are devices like smart watches to trace the heart rate, glucose level for diabetics, sleep time duration, workout results, breathing rate, body temperature and other health indicators. These indicators can be shared either with different applications to create an overview of our day or with the doctor [2], who can adjust medical treatment according to the received information.

In retail shops they use different sensors, lasers and RFID scanners to improve their business strategy by better supply chain management and creating customer's profile. According to the study of [3] the improved store performance, choice of products and customers footprint can be measured by the means of indoor positioning system.

Table 1 (see Table 1) created by the author shows the existence of the problem about customer's personal information in regards to every type of smart device. According to Table 1, certainly, there are many different ways to make life or business process easier, and people continue looking for different ways to implement the Internet of Things technologies in other industries. Thus, the trend of Internet of Things will be constantly growing.

3 Privacy limitations and Solutions

Privacy is a very important aspect of human's life, especially when all devices people are using, sometimes are able to collect sensitive information about our life. The Internet of Things devices create information that is used for the analysis purpose [4].

All devices in the Internet of Things generate data, and not all people understand what happens after they agreed with all the terms and conditions proposed by the business. Users have limited rights in managing smart devices. According to the study [5], in order to use the collected data user permission should be acquired stating what opportunities this data will make for the future use of this technology.

Proceedings of the XX International Conference "Data Analytics and Management in Data Intensive Domains" (DAMDID/RCDL'2018), Moscow, Russia, October 9-12, 2018

Table 1 The existence of the problem about customer's personal information

Type of smart device	What for	Personal data leak issue	Type of Information
Smart control	control monitoring the status and the mode of home devices	Exists	Status, mode
Smart power-saving	evaluates the user energy consumption patterns and assists in reducing the waste of energy	Exists	Water amount, gas amount and electricity amount in a certain period of time
Smart application	potentially expand the functionality of home's smart devices	Exists	Vulnerabilities in the software
Smart transport	real time traffic control, remote diagnostics, logistics automation	Exists	No data
	for better route selection and accident reports	Exists	Information exchange between the cars (multihop)
Smart Ecology	Air Quality Egg o monitor the air quality and pollution level in the city and create a pollution map	No	No data
Smart health industry	medical data from smart health devices, medical supply management	Exists	Exchange of health data with doctors, adjustment of treatment
Retail shops	Evaluate the business strategy	No	No data

Next four subsections will discuss how to limit the possibility of a hacker attack and other vulnerabilities. An in-depth literature review has been made to categorize many different types of vulnerabilities for future implementation and modeling in the research stand.

3.1 Solution One – Light weight authentication method Numerical Control Information

The Internet of things sensors, application and services are usually connected by a software-defined networking controller. This technology makes network control easier by dividing network flow of the control plane from the data plane. But the issue with this technology is that none of the existing controllers have security firewall to block malware containing packets from reaching the device manager [6]. Current situation makes the privacy control questionable in different smart devices.

3.2 Solution Two – Controller with enhanced security firewall method (Data security and data encryption)

Privacy question is very sensitive for people. More than 60% of social media users identified the lack of control on shared information [7]. People are using web security surveillance IP-cameras inside their apartments, but when people are at home, they continue recording, and that makes their life more transparent. Someone who has access to their Wi-Fi network can use man-in-the-middle breach to gain unauthorized access to video archives or can open the door lock. Attacker, who got access to private medical data held on smart health devices or got permission level to change the code of the mechanisms, can potentially cause major health problems or even death [8].

3.3 Solution Three - Data encryption both local and in the cloud

If the data from the smart devices will be stolen and misused, *it will have a big impact on privacy*. Different companies, such as social networks, smart phones, laptops, some loyalty programs and other have total overview of our life since 2010, they know what people buy, where do they spend time and even how do they look, because of recent implementation of face recognition systems into our phones, tablets and laptops. Local Internet providers are sharing Internet usage information, such as cookies with different advertisement organizations.

Technologically advanced world makes people's life easier, but at the same time increases the dependence on the used systems. As mentioned in the article by [9], the autonomous vehicles are very dependent on the infrastructure, and if some part of the infrastructure has failed, because of the weather condition or a hacker attack, appears an unforeseen time gap between autonomous driving and driver's involvement, because they lose connection with out of sensor range neighbours. Market leaders create smart device ecosystems, which don't have a proper security implementation.

One example, in March 2018 Amazon has bought a door bell system for 2 billion dollars. After implementing it with Amazon Alexa they will have access to the information about people, who are currently at home or who went on vacation.

3.4 Solution Four– Anonymizing data

All these technologies are reducing privacy around the globe, and if the access to the information is not managed properly it can result in increase of criminal actions and privacy violations in the future and subsequently limit the usage of the Internet of Things. People can just accept the fact they are being watched and somebody has access to their life. Any business is interested in income, and lack of attention to security measures may potentially turn into problems with personal privacy and data information security. If the Internet of Things data gets compromised different consequences may happen. The future privacy limitation is an expanding problem, which will be discussed further.

4 The level of personal information security

The Internet of Things devices generate very large amounts of data every day. All this data is accumulated, transferred, stored and analyzed. As more devices will be sold, the more attractive this data will become for hackers. The level of security of smart devices is usually very poor. According to research of [10], one of the problems is in numerical control information. Numerical control information in Internet of Things is about how devices interact with each other. Access to the privacy information can be obtained because of false routing or a replay attack. According to the study of [11] personal information can contain names, address, phone numbers, emails and others. The damage from the loss of personal information refers to the violation of both business and customers interests in the disclosed information.

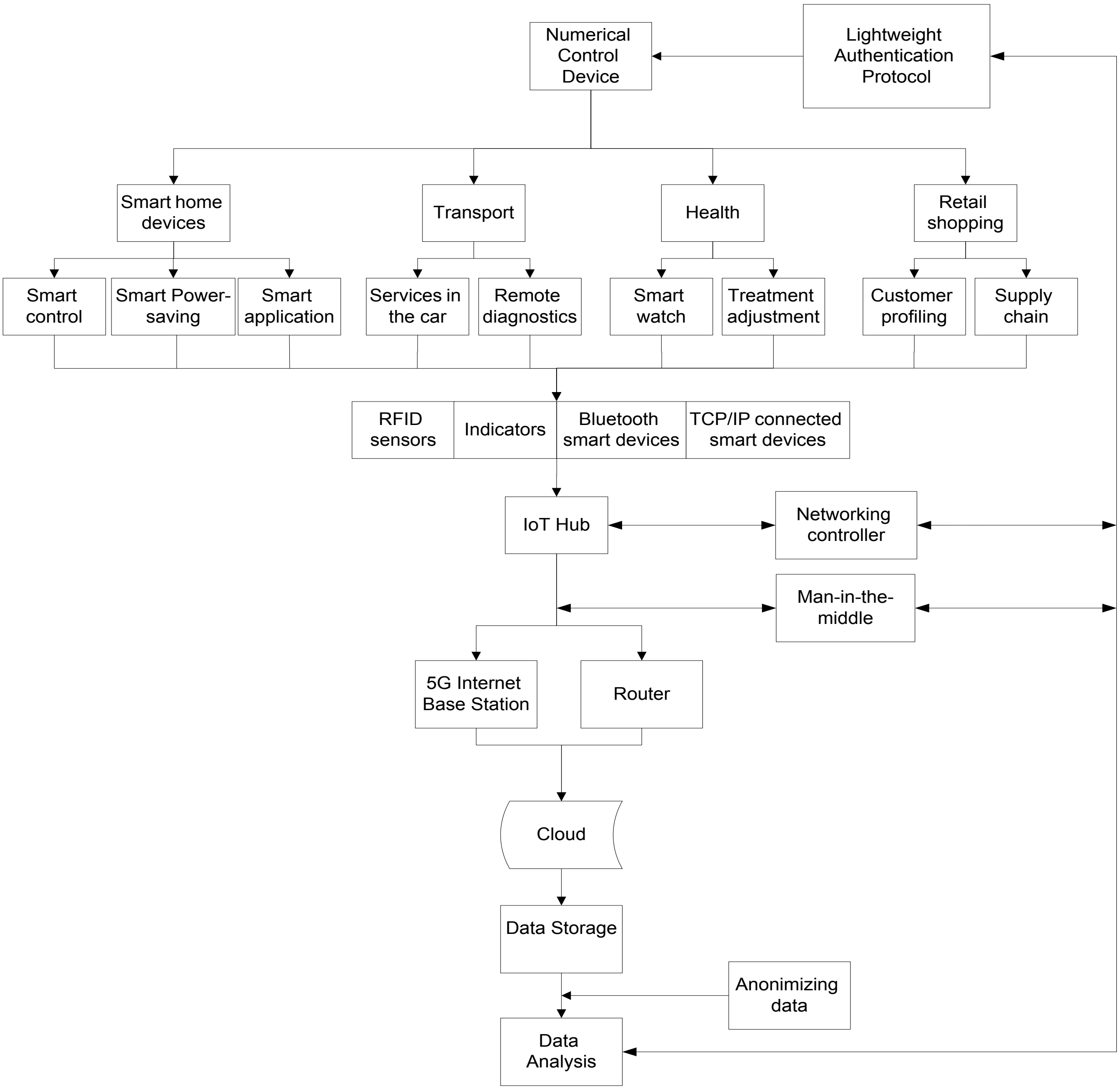

Figure 1 Scheme of Research Stand

The purpose of this paper was to prepare research stand aimed to the privacy limitations and security analysis in the Internet of Things using the content of the Table 2 (see Table 2), it describes the Problems and Solutions of the IoT, as a summary of the previous section.

Table 2 The aspects of the security of Internet of Things

Problem	Solution
Low level of personal information security	Numerical Control Information
Low level of the privacy control	Networking controller with enhanced security firewall
Data theft and misuse	Anonymizing data
Authentication process in transfer control between the Internet of Things devices	A transfer security lightweight protocol

Each problem is planned to be analyzed in regards to the level, where the vulnerability may occur. During the modelling process [12], sample data will be sent to the IoT hub and different analysis and characteristics of the problem will be measured at the solution implementation point to verify the proposed stand structure and to recommend possible solutions to eliminate gaps in security.

Conclusion - Future DID's Impact on Privacy

The topic identified for further research is data intensive analysis in DID**.** Different types of the privacy limitations' and solutions' are briefly described further and illustrated by Figure 1 (see Figure 1) Scheme of Research Stand. Different levels of dataflow are presented on the scheme. First level is showing the industries and types of implementation of the IoT. The second level shows examples of data collecting methods. The third level from IoT hub to Data Analysis shows the process of collecting and processing the data and types of vulnerabilities, which may affect the security. Each of the solutions on the scheme gives an illustration of every solution for better understanding, on which level each of them may be tested and what other new possible outcomes can be foreseen during the dataflow.

Acknowledgments. This work is supervised by Associate Professor, PhD, Dr. Elena Smirnova, Faculty of Informatics and Control Systems, Bauman Moscow State Technical University.

References

[1] Ko, J., Lee, B., Lee, K., Hong, S., Kim, N., & Paek, J. (2015). Sensor virtualization module: Virtualizing IoT devices on mobile smart phones for effective sensor data management. *International Journal of Distributed Sensor Networks*, *2015*, 1-10. doi:10.1155/2015/730762

[2] Buldakova, T.I., & Suyatinov S.I. (2014) Reconstruction method for data protection in telemedicine systems // Progress in Biomedical Optics and Imaging - Proceedings of SPIE. 2014. Vol. 9448. Paper 94481U.

[3] Hwangbo, H., Kim, J., Lee, Z., & Kim, S. (2017). Store layout optimization using indoor positioning system. *International Journal of Distributed Sensor Networks*, *13*(2), 27-40. doi:10.1177/1550147717692585

[4] Perera, C., Zaslavsky, A., Christen, P., &Georgakopoulos, D. (2014). Context aware computing for the Internet of Things: A survey. *IEEE Communications Surveys & Tutorials*, *16*(1), 414-454. doi:10.1109/surv.2013.042313.00197

[5] Perera, C., Ranjan, R., Wang, L., Khan, S., &Zomaya, A. (2015). Big data privacy in the Internet of Things era. *IT Professional*, *17*(3), 32-39. doi:10.1109/mitp.2015.34

[6] Nguyen, T., &Yoo, M. (2017). Analysis of attacks on device manager in software-defined Internet of Things. *International Journal of Distributed Sensor Networks*, *13*(8), 44-52.doi:10.1177/1550147717728681

[7] Sarikakis, K., & Winter, L. (2017). Social media users' legal consciousness about privacy. *Social Media + Society*, *3*(1), 1-14. doi:2056305117695325

[8] Khera, M. (2016). Think like a hacker. *Journal of Diabetes Science and Technology*, *11*(2), 207-212. doi:10.1177/1932296816677576

[9] Lee, E., Gerla, M., Pau, G., Lee, U., & Lim, J. (2016). Internet of vehicles: From intelligent grid to autonomous cars and vehicular fogs. *International Journal of Distributed Sensor Networks*, *12*(9), 1-14. doi:10.1177/1550147716665500

[10] Li, Y., & Li, M. (2017). A privacy protection mechanism for numerical control information in Internet of Things. *International Journal of Distributed Sensor Networks*, *13*(8), 16-24. doi:10.1177/1550147717726312

[11] Lu, X., Qu, Z., Li, Q., & Hui, P. (2015). Privacy information security classification for Internet of Things based on internet data. *International Journal of Distributed Sensor Networks*, *11*(8), 11-17. doi:10.1155/2015/932941

[12] Buldakova, T.I., & Dzhalolov A.S (2012). Analysis of data processes and choices of data-processing and security technologies in situation centers // Scientific and Technical Information Processing. 2012. Vol. 39. No. 2. P. 127-132.