Privacy concerns in IoT smart healthcare system

Milan Stojkov*, Goran Sladić*, Branko Milosavljević*, Miroslav Zarić*, Miloš Simić*
* University of Novi Sad, Faculty of Technical Sciences, Novi Sad, Serbia
* {stojkovm, sladicg, mbranko, miroslavzaric, milos.simic}@uns.ac.rs

***Abstract* — Internet of Things has been changing the world in the last couple of years with a tendency to have an even bigger impact. In the beginning, the vast amount of data was collected, processed and stored in the cloud. Now, more and more of these operations are done on the IoT devices with respect to their limitation in terms of storage and processing power. The responsibility is transferred from the cloud to the IoT devices and that fact raised big security and privacy concerns that can lead to different problems like disclosure of the user's identity or device location. In this paper, we identify different groups of privacy issues that can occur and try to tackle them through a simple smart healthcare scenario where we propose different solutions for detected issues.**

Keywords: Internet of Things, IoT, privacy, privacy patterns, smart healthcare

I. INTRODUCTION

Internet of Things is rapidly getting more attention of academia and industry and it is not considered as a new concept of computing anymore. The estimated number of 50 billion ubiquitous and interconnected devices by the year 2020 is proof of that [1]. The rapid expansion of the IoT concept can be explained by its flexible nature to be applied to different domains such as smart cities, smart healthcare, home automation, logistics and transportation, smart grid, etc. In the beginning, the IoT ecosystem was relying on a very powerful computing infrastructure built in the cloud [2]. Today, the IoT architectures are more heterogeneous than ever before, and as the complexity grows, new concerns emerge. Major issues are still related to performance, while other issues like security and privacy are not getting enough attention, but the situation is improving. Data security and privacy are huge obstacles to the widespread application of the IoT systems. The fear that sensitive information will be lost or exposed is the main reason why so many people still postpone the adoption of this kind of technology. Therefore, the protection of user data and privacy is a driving factor in determining the efficiency and viability of the IoT [4]. In this paper, we want to identify and tackle privacy problems that can occur in IoT systems.

The rest of the paper is organized as follows: Section II presents related work in the field of privacy in IoT. Section III gives a brief overview of privacy in IoT. In Section IV we give a classification of privacy issues and mapping of detected privacy issues on appropriate classes. In Section V simple smart healthcare system is analyzed in terms of privacy issues earlier detected and solutions are proposed relying on appropriate privacy design patterns. Section VI discusses the finding and concludes the work.

II. RELATED WORK

There is an increasing number of papers that deal with security and privacy in IoT. Some of them only give a brief overview of privacy in IoT [3]. Different papers usually focus more on security than privacy, and some of them even consider privacy as part of security [11]. The work in [11] defined privacy and emphasized the control of enhancing user's privacy. One of the papers this research relies upon is written by Abi Sen et al. [6] where authors define a fine-grained list of approaches and techniques that are used to fulfill the privacy requirements. This fine-grained list was a starting point for defining more coarse-grained groups of privacy issues that are more appropriate for the architecture of IoT systems and easily expandable. Authors in [10] discussed the importance of having a separate Privacy Policy Agreement (PPA) for IoT devices as it differs from website PPAs and directly influences which privacy patterns should be applied.

Although these researches have contributed to many privacy issues in IoT we have not found an approach that would combine security and privacy by design from the architectural point of view. This paper attempts to fill this gap.

III. PRIVACY IN IOT

According to the Internet Security Glossary, data privacy is described as "the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others" [5]. Certainly, security is an older concept that tries to provide mechanisms for the protection of devices and data from different types of inner and outer attacks where manufacturers are more turned to the defense of the software and hardware they produce than users. Privacy as a term puts more emphasis on the user and misuse of user's data. If we mention the fact that the General Data Protection Regulation (GDPR) or Health Insurance Portability and Accountability Act (HIPAA) are already effective, security and privacy as terms should be separated. As a result of the separation, more emphasis should be put on designing privacy-friendly services and establishment of the concept called privacy by design. These regulations give strong parameters what can and cannot be put in place to keep an entity compliant, but when it comes to IoT devices and platforms there is a bit of grey area. Those companies that are working in a partnership or some sort of relationship with an official entity, such as a health system of one country, are clearly covered under regulations that are set in place. But for consumer goods that deal with health data but are not

Copyright 2019 by Information Society of Serbia - ISOS, Serbia | Creative Commons License: CC BY-NC-ND

TABLE 1 PRIVACY ISSUES CLASSIFICATION

Perception layer	Network layer	Application layer
Collection of more data than required without user consent	Disclosure of user's identity	Disclosure of user's personal information
	Disclosure of user or device location	User's movement analysis
Data and device tampering	Data tampering	Behavioral analysis
		Lack of digital forgetting

directly linked to healthcare entities under appropriate regulations the lines are a bit blur. For example, you can purchase FitBit smart fitness device at Amazon that is used to loosely monitor activity levels without any relation to a healthcare provider, but these data can be used as health data that can be processed further.

Different authors have different approaches for tackling privacy issues – starting from unstructured enumeration of detected issues to grouping of privacy issues by some criteria, e.g. based on types of attacks or data being used. Our approach uses the advantages of the IoT multi-layer architecture and naturally groups the issues that can occur on each layer. In this way, two important approaches can be combined (security by design and privacy by design) and result in a more secure solution. Also, we investigate how the different characteristics of IoT architecture could be used to improve users' privacy.

IV. CLASSIFICATION OF ISSUES IN IOT

The vast amount of research concerning privacy only mentions different issues without giving proper classification or structure. Since any unstructured list of issues would only expand further, manufacturers of devices or applications would have to adjust to the never-ending lists of potentially not applicable issues for them. That is why different approach has been made to group the most relevant issues into familiar groups that can be used during system design. Additionally, these privacy issues are crossed with different privacy design patterns [7] that offer solutions that are applicable in IoT systems. Different research showed that the IoT can be considered as multi-layer architecture which is roughly divided into three layers:

- perception layer,
- network layer (with support services), and
- application layer.

For mapping specific privacy issues on different layers, we first had to detect those that are most commonly mentioned or further discussed in different research. Therefore, we did a comprehensive literature review by examining the electronic database Google Scholar. By using the snowball and cross-referencing methodology we extracted the most common privacy issues that are mentioned in papers. We considered only papers written in English that contained an abstract and were published between 2010 and 2018. We conducted this review using search terms "privacy", OR "privacy issues", OR "privacy challenges", OR "privacy concerns" combined with "IoT" (or Internet of Things). We screened the abstracts and titles of the filtered papers and found that the majority of them combines the security and privacy issues. By adding the search term "eHealth" (and similar terms, such as Telehealth, mHealth, uHealth, smart healthcare) we managed to narrow the result to below dozen relevant, mostly conference papers.

With that in mind, we grouped different privacy issues found onto three layers as presented in Table 1.

On the perception layer we have two major issues:

- collection more than required data without user consent – some of the major IoT manufacturers are not adhering to their own PPAs on data being collected [10] which is the reason the clear majority of people are still not deciding to use smart devices regularly.
- data and device tampering – tampering with data is clearly security and privacy issue that is easily done on primitive devices that exist on the perception layer and that can affect the whole communication in the system. This includes even replacing the original device with a malicious clone.

On the network layer the following issues can emerge:

- disclosure of a user's identity – user's identity is often not encrypted during the transport that was easily detected using network sniffing tools [10]
- disclosure of user or device location – besides the user information, location can be considered one of the most valuable information that can be collected since the common data that is being sent by the devices consists at least of location, data/query, and user's ID.
- data tampering – a little bit harder than on the perception layer, but still a major issue

Finally, on the application layer we have:

- disclosure of user's personal information – any kind of disclosure of personally identifiable information (PII) can be considered of violation of main privacy requirements.

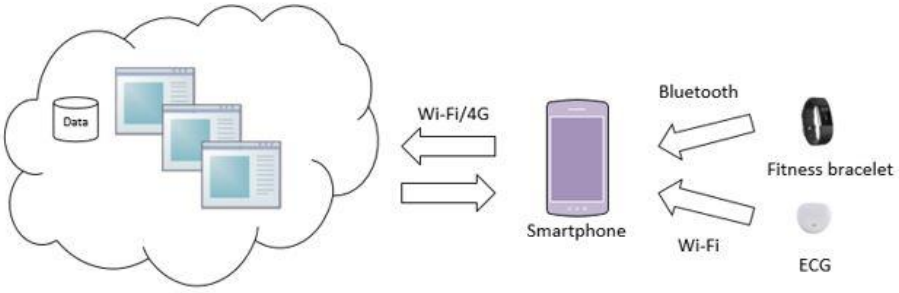

Figure 1. System architecture

- user's movement analysis – this analysis can negatively affect a user's privacy by detecting the user's movement and location and making further predictions and tracking.
- behavioral analysis – certain patterns of default user's behavior can be detected. This can be closely coupled with the user's movement analysis.
- lack of digital forgetting – HIPAA, GDPR, and other regulations clearly state that this is one of the basic rights for every human and lack of providing this option is clearly an issue.

The number of potential issues is expanding with the level of intelligence of the layers with the application layer having the most issues detected. Every of detected privacy issues can be mapped on appropriate privacy design pattern and tackled accordingly. Evaluation of these privacy issues with solutions is done on a smart healthcare scenario.

V. SOLUTION

In order to demonstrate the proposed classification of privacy issues and the applicability of privacy patterns, we assumed the existence of a simple scenario where smart healthcare architecture is presented in Figure 1.
The system consists of the following:

- Smart tracking fitness devices and smartphones with ECG devices as sensors that can detect health problems such as a stroke or heart attack
- The smartphones that act as an IoT gateway that collect information from the sensing devices and send the information to the cloud service. Smartphones can be gateways for patients and doctors as well.
- Cloud services with appropriate database responsible for data collection, analysis, monitoring and alerting

In this scenario, we can recognize most of the privacy issues earlier classified into three groups and elaborate findings.

A. Perception layer issues

On the perception layer, we have different devices that collect data. These devices usually come with applications in mobile of web form with which they interact. Thus, the users must be familiar with the data devices and applications collect. This can be regulated with an adequate privacy pattern. Concretely the following privacy patterns can be applied:

- Privacy policy display – this pattern defines that it should be clearly stated what information is needed by whom, for which purposes, and by what means, prior to soliciting consent which is of big importance to patients.
- Privacy-aware wording with Abridged terms and conditions and Layered design – this patterns state that privacy-related information should be presented using low difficulty vocabulary with short concise sentences to persuade the user to process it. Also, the Terms and Conditions must be summarized into concise and relevant information with the most crucial aspects of the privacy policy extracted since the user's attention cannot be kept for a very long time.

For the data tampering on this layer to happen, physical replacement of the original node with the malicious one is a common scenario that can happen. That is why we have to have some solution for preventing this for example by implementing a multi-step process for secure registration of nodes as mentioned in [9].

B. Network layer issues

Cyr et al. [8] applied a security test on the Fitbit Flex fitness device and found that sensitive information such as the BLE credential is sent in plaintext from the Fitbit web server to the smartphone application. This means that the attacker can obtain this information via a Man-in-the-Middle attack. Also, smartphones can eavesdrop nearby Fitbit devices and send their MAC addresses to the Fitbit server which can allow anyone to track other Fitbit users, make user's movement analysis, etc.

Message format in the IoT systems is not standardized and that implies different data tampering techniques can be applied. The common data that is being sent by the devices consists at least of location, data/query, and user's ID. This can be considered as PII that should not be transferred in plaintext.

The following privacy patterns can try to solve three mentioned issues:

- Encryption with user-managed keys – this pattern defines that encryption of

the PII must be done prior to storing or transferring. In this solution the user generates a strong encryption key and manage it themselves, away from untrusted online services or 3rd parties.

- Onion routing – this pattern states that data must be encrypted in layers such that every station on the way can remove one layer of encryption and thus get to know only the immediate next station. The goal of this pattern is to achieve unlinkability between senders and receivers which can be used for sending eHealth data for anonymous statistical purposes or making an anonymous diagnosis by the doctors.
- Aggregation gateway – this pattern can be used when detailed measurements which are linked to the user should modify service operations at each moment according to the data sent. These measurements may reveal further information when repeated over time, so the pattern suggests the usage of homomorphic encryption to establish reliable access to the aggregated data load at every moment. This can be used to generate rules for alerting the ambulance in emergency cases without revealing information about e.g. personal habits.

C. *Application layer issues*

On the application layer, we have the issues that are not new, since they are already familiar in cloud environments. Thus, a great number of patterns can be applied. Since that is the case, we propose the following patterns should be applied from the device and communication perspective where the small amount of data is actually handed over to applications for them to process:

- Protection against tracking - cookies, and tokens carrying any form of PII should be deleted on a regular basis.
- Personal data stores - cloud services should not store all the user's data, but the data should be under the control of the user where smartphones would be considered as the personal data stores that store encrypted information and send the only minimal amount of data to the cloud
- Selective access control – users must have the option to define the audience which can use their data by specifying the access rules to their data.
- Added-noise measurement obfuscation - any data sent to the cloud services for analytics should also be obfuscated and should decouple content from the location information.
- Decoupling content and location information visibility – the goal of this pattern is to avoid that one service learns characteristics about the users, especially their location if this is a peripheral service which does not need that kind of information.

VI. CONCLUSION

In this paper, we addressed the problem of privacy in IoT systems. We proposed a coarse-grained classification of issues based on architectural layers. Detected privacy issues were mapped on appropriate privacy design patterns for IoT and discussed in a smart healthcare scenario. The other application domains can benefit from this research such as different industrial systems or smart grid. Of course, not all familiar patterns can be applied in every case because of the certain properties of the IoT systems. Due to the nature of the sensing devices and their constrained power, there is not always room for sophisticated encryption techniques or power consuming processing.

In future work, we will address privacy issues on the application layer in more detail, especially how they relate to other privacy issues already detected in the cloud SaaS solutions. Also, we will try to propose new privacy patterns that can potentially solve the problems that can occur in this kind of constrained environments.

REFERENCES

[1] Evans D., The Internet of Things How the Next Evolution of the Internet Is Changing Everything. Online White Paper. https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. Accessed December 20, 2018

[2] Botta A., de Donato W., Persico V., Pescape A. Integration of Cloud computing and Internet of Things: A survey. Future Generation Computer Systems, 2016, Volume 56, pp. 684-700.

[3] Atzori L., Iera A., Morabito G. The internet of things: a survey. Comput Netw, 2010, doi:10.1016/j.comnet.2010.05.010

[4] M. Abomhara, G. M. Kien. Security and privacy in the Internet of Things: Current status and open issues, 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), 2014, pp. 18.

[5] Internet security glossary. https://www.ietf.org/rfc/rfc2828.txt, 2017. Accessed December 20, 2018

[6] Abi Sen, A.A., Eassa, F.A., Jambi, K. et al. Preserving privacy in internet of things: a survey. Int. j. inf. technol. (2018) 10: 189.

[7] Privacy Patterns Website. https://privacypatterns.org. Accessed December 20, 2018

[8] B. Cyr, W. Horn, D. Miao, M. Specter. Security analysis of wearable fitness devices (Fitbit). Massachusets Inst. Technol., p. 1, 2014.

[9] Stojkov, M., Simić, M., Sladić, G., Milosavljević, B. Two-step process for secure registration of nodes in IoT systems. In: Konjović, Z., Zdravković, M., Trajanović, M. (Eds.) ICIST 2018 Proceedings Vol.1, pp.28-31,2018

[10] Subahi A., Theodorakopoulos G. Ensuring Compliance of IoT Devices with Their Privacy Policy Agreement 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), Barcelona, 2018, pp. 100-107.

[11] Borgohain T., Kumar U., Sanyal S. Survey of security and privacy issues of internet of things. 2015. arXiv:1501.02211

[12] Ziegeldorf, J. H., Morchon, O. G., Wehrle, K. Privacy in the Internet of Things: threats and challenges. Security and Communication Networks. 2014, 7(12), 2728–2742. doi:10.1002/sec.795