A Framework for Privacy Policy Compliance in the Internet of Things

Constantinos Ioannou(✉)

Centre for Secure, Intelligent and Usable Systems,
University of Brighton, Brighton, UK
c.ioannou1@brighton.ac.uk

Abstract. Internet of Things (IoT) structures are pervasive, incredibly complex, heterogeneous, based on various architectures and infrastructure. IoT exposes users to a number of different privacy threats that are related to leakage of personal information and loss of service. User privacy is the most important aspect of IoT environments as user's data are transmitted among connected devices without user's intervention. Therefore, the challenges that IoT privacy and security analysts are facing is relating to having difficulties to analyse and design such complex, heterogeneous systems by guaranteeing the protection of the exchanged user data. Accordingly, tools to support and guide the analyst are needed, in order to make them to design IoT systems that are compliant with privacy policies. In this paper, preliminary results are provided for designing a tool-supported, theoretical framework, including a privacy policy language and a model for the analysis of IoT systems to enforce the protection of user data in IoT environments. In this work, the literature review is illustrated for identifying the concepts and relationships needed for such a framework, an outline our preliminary design of it and the included components.

Keywords: Internet of Things · Privacy engineering · Security engineering · Requirements engineering

1 Introduction

Internet of Things is defined as "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment." [1]. IoT has several fields of use where it can provide really valuable services, including healthcare, transportation, infrastructure and home. Sensors and wearable devices could be used in healthcare to monitor patients and senior citizens' medical conditions, help drivers to become fully aware of driving conditions and in a home setting there are various operations to automate task such as temperature control, lighting, multi-media, window and door operations etc. It is a collection of devices attached to the Internet that

F. Dalpiaz et al. (Eds.): RCIS 2020, LNBIP 385, pp. 595–603, 2020.
https://doi.org/10.1007/978-3-030-50316-1_43

uses nodes (a node is a connection point that can receive, create, store or send data along distributed network routes) and controllers to collect and exchange data.

Madakam, S et al. define IoT as [2] "An open and comprehensive network of intelligent objects that has the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment".

Internet of Things is an emerging technology and is designed to support any device without regard to its software, hardware or even supported protocols. There are possible opportunities of attacks (also known as attack surface) as IoT expands and more devices join the network. There are many issues with IoT Devices as most of them are mass-produced and are similar in design, which means one attack can be executed in multiple systems. Additionally, many IoT Systems are poorly designed and implemented, using diverse protocols and technologies that create complex configurations.

Security scientists have found increasing weaknesses in several IoT systems which could have been avoided by taking account standard security measures throughout the development phase [3]. Throughout implementation, the action of performing security analysis, guarantees that the end product fulfils particular security standards. Applying secure practises early in the development cycle, is a method recommended by the area of requirements engineering. Requirements engineering modelling is conducted by specifying the specifications of the actors in the development process in order to achieve security requirements.

Thus, this project work is focused on a privacy framework to design and analyse IoT systems by introducing a model-driven approach. A modelling language would be developed to model an IoT system. The modelling language, will include the characteristics with which define a model of an IoT system. The system's privacy posture could be analysed depending on the model's details. The method of analysis will be formalised through a collection of algorithms. The algorithms will introduced in a software tool which supports the Framework application. Concepts defined are used to build a modelling language in the area of diagrams, to construct modelling cases of IoT systems.

The framework uses concepts from the areas of study of security and privacy requirements engineering. The concepts defined are used to build a modelling language in the context of diagrams, to construct modelling cases of IoT systems.

The rest of the paper is as follows. In Sect. 2 the Research Challenges and Questions that are derived from the literature. In Sect. 3 the Literature Review illustrates preliminary results extracted from the evaluation of existing frameworks. Finally, in Sect. 4 a proposed solution that will be implemented in the future is outlined.

2 Research Challenges and Questions

IoT applications have a range of characteristics and challenges to analysis that emerge at various levels. From creating an IoT framework to implementing it and maintaining its life cycle.

An important challenge faced with IoT is the interoperability [13], as there are heterogeneous and decentralized IoT networks for the distribution and utilization of range of informations and services. Interoperability is a characteristic of IoT system that should be articulated in a modelling language.

Equally important challenge is the identification-based connectivity that is developed between a thing and the IoT system, depending on the identification of the thing [14]. IoT applications are required to communicate to networks that provide user's credentials without their assistance. In IoT contexts, at the production phase, identifiers of a device could be given. Consequently, an identifier of an object is a resource element included in the language of modelling.

Strong-level privacy challenges relate to the linked complexity of a "thing" that leads to major security threats, including disclosure threats, authenticity, data and services dignity as well as confidentiality [15]. This drives to the result that a modelling language requires to express threats and vulnerabilities.

Likewise, manageability challenges should be tackled using formal processes at the modelling level, as IoT applications mostly of the times work automatically without human intervention [16].

IoT is unique in the fact that it incorporates traditional and robust technology with modern untested technology. The combination of developed technology with new technology leads to security and privacy concerns. Due to the unique complexities, IoT's existing solutions face the main objective of the research, which determines to what degree an engineer in IoT systems can extract security as well as privacy requirements. The prior argument could be broadened to the following questions of research:

2.1 Research Questions

- **(RQ1) Research Question 1:** What are the core aspects of privacy specification for an IoT network?
- **(RQ2) Research Question 2:** What existing Privacy Requirement Engineering (PRE) tools capture privacy concepts and are they applicable for the Internet of Things environments?
- **(RQ3) Research Question 3:** How can we coherently model IoT privacy and what are the required components of a modelling language to elicit IoT Privacy Requirements?
- **(RQ4) Research Question 4:** How can we check compliance of IoT systems with privacy policies?

Starting from **RQ1**, a comprehensive and detailed analysis of the literature was conducted. The literature review was performed to recognize IoT's unique characteristics including relevant IoT Privacy issues. Furthermore, Privacy Requirements Methodologies will be investigated towards deciding if they are applicable to IoT. This will be helpful to understand the difference between traditional Privacy Requirements Engineering practises and developers' privacy practises in the context of IoT in order to resolve **RQ2**. Accordingly, a conceptual model which will be a part of a privacy framework will be proposed in order

to tackle **RQ3**. The main components of the IoT Privacy Framework will be the Terminology used to address terms which classify the concepts of the privacy framework suggested. The terminology would encourage the reasoning regarding an IoT system's privacy by creating a language between privacy engineers. The Modeling language which offers elements for constructing an IoT system model which collects the information that privacy engineer requires to conduct an IoT system's privacy analysis. The conceptual model, language semantics, and language notation will be part of the modeling process. The methodology used to create model instances of an IoT system for requirements elicitation by security engineers. The methodology will include guidelines along with limitations on how modelling instances are generated using the modeling language. Lastly, to address **RQ4** which extends RQ3 an analysis processes will be employed on models and formalized. After the formalization is done, a case study will be used to evaluate and check compliance or non-compliance of IoT systems with security and privacy policies.

3 Research Methodology

The purpose of this study is to develop a deep knowledge of the concerned area with a reference to solving these issues, therefore a design-science research methodology (DSR) [17] will be used. DSR will be applied to the problem area as it is a dynamic problem-solving paradigm. It provides a simple step-by-step approach which can be adopted in any project of information technology. This method's approach is to define particular issues as well as provide novel and practical solutions using four artifacts: frameworks, models, methods and implementations. Once a problem is identified, an artifact is developed to provide a solution. The artefact, in this case, will take the form Framework for Privacy Compliance in IoT.

4 Literature Review

A quantitative Systematic Literature Review (SLR) was carried out to establish the current progress reported in the literature on approaches (methodologies, policies, etc.) that support Internet of Things privacy-awareness [18]. To identify relevant works for this review, several selection criteria have been set. Firstly, for an article to be considered appropriate, it needed to rely on both the overall area of privacy and IoT. Given that the overall emphasis of this research is on developing of IoT system's privacy, modeling is a crucial factor to be considered. The studies found required to be under the scope of model-driven engineering and include "model-driven" methods to the design of IoT systems to be included in the study. This study avoided methods such as algebraic modelling or any other mathematical methods. Papers that were published in academic journals were obtained from freely accessible scholarly literature search engines and digital libraries such as Google Scholar, IEEE, Research Gate, SCOPUS, Springer and Science Direct. The keywords used for our searches were "internet of things

privacy", "internet of things challenges", "privacy requirements engineering", "model-driven" AND "IoT Privacy", "IoT*" AND "privacy requirements engineering".

To achieve complete overview of the research area, a preliminary literature review was performed to address Research Questions 1 and 2 for identifying concepts for designing a language for privacy policy compliance.

The literature presents us with privacy frameworks which are used to obtain system privacy requirements. IoT is an area which includes specific requirements and specifications. A privacy framework should be able to fulfil IoT characteristics and requirements as mentioned in the Fig. 1, in order to be applicable for security and privacy analysis. The preliminary evaluation of the frameworks regarding the criteria is presented in Fig. 1).

Criteria	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]
Access control	-	✓	-	✓	✓	✓	✓	✓
Anonymity	-	-	✓	-	-	-	✓	✓
Consent	-	-	-	-	-	-	✓	-
Data Disclosure	-	✓	✓	-	✓	-	-	-
Data minimization	-	-	-	✓	-	-	-	✓
Openness and transparency	-	✓	-	✓	✓	-	-	✓
Safeguard and remedies	-	✓	-	✓	✓	-	-	✓
Data Lifespan	-	-	-	-	-	-	-	-
Autonomy	-	✓	-	-	-	-	-	-
Error Handling	✓	-	-	-	-	-	-	-
Adaptive	✓	-	-	-	-	-	-	-
Run-Time Adaptation	✓	-	-	-	-	-	-	-

Fig. 1. Evaluation of frameworks

The primary motivation behind the growing interest in policy-based services, networks and security systems is to facilitate flexible adaptability of behaviour by changing policy without coding or stopping the process. This indicates that it should be feasible to dynamically alter policy rules interpreted by the decentralised entities in order to adapt their behaviour.

Policies are extracted from goals and objectives, service level agreements or trust relationships within or between entities. The refining of such conceptual policies into policies referring to specific services and then into policies that can be implemented by specific service-promoting devices is not easy and can not be automated effortless.

Nonetheless, several efforts were made from a privacy and security perspective to resolve the security and privacy concerns. Certain academic studies recognise IoT security and privacy threats and recommend potential approaches for security researchers.

In their work "A Context-Based Behavioral Language for IoT" [4], the authors, proposed the use of scenario-based programming approach and specifically the graphical language of live sequence charts (LSC). This addresses one aspect of the specification growth issue by allowing a natural break-down of the specification in alignment with the requirements. The other aspect of their solution, aiming at further simplifying and shortening the specification, is based on subjecting these scenarios to context–a key concept in IoT and autonomous robot modelling. Their modelling language must be adaptive and facilitate systematic development as the specifications are typically not known in advance and improvements would be made on an ongoing basis. Also, it should have formal semantics, allow the specification of a generic functionality and support error handling.

In this paper [5], a framework for ethical requirement elicitation eFRIEND with automated reasoning is combined. In order to provide vulnerable users with trustworthy and secure IoT in healthcare contexts, they have to implement ethics in order to meet acceptable system requirements. Their project address key principles such as accessibility, data protection, reliability, transparency, and autonomy.

Aivaloglou, Gritzalis and Skianis [6], identified a set of requirements for the development of sensing network that are aware of privacy. The suggested model was developed from an awareness based on data security standards including privacy issues. This recommendation proposes five concepts that are focused on sensor networks, the foundation for the creation of omnipresent IoT-based solutions that carry higher privacy risks.

In May 2008, a detailed privacy and security policy was published by the Center for Democracy & Technology [7] to promote health data protection. This framework is a modified version of the Common Framework published by the Markle Foundation in the Connecting for Health (Markle Foundation, 2008) initiative. The framework includes 9 concepts based on a combination of legislative action, policy and engagement from industry.

The U.S. National Health Information Technology Coordinator's Office (Local Coordinator's Office, 2008) [8] also implemented a standardized system for the digital sharing of personally identifiable information. A systematic study and evaluation of these concepts were carried out by taking into account as many differences as possible while also keeping in mind how they can be applied to electronic data. The ONC framework incorporates eight principles which act as guidance for public and private sector organizations keeping or sharing individual health-related electronic data and helping direct the implementation of health information technology by the government.

Alqassem and Svetinovic [9] published a taxonomy on the IoT's criteria for security and privacy in 2014. In an IoT smart grid case, the taxonomy provided value characteristics which were enforced. The paper provides support for further review of IoT-related vulnerabilities and threats to the expected privacy and security. The four concepts mentioned specifically address IoT's security aspects.

Recently, in the scope of disabled people, AL-mawee [10], published a survey of security and privacy concerns in IoT healthcare applications. There has been a broad range of IoT-based applications for the elderly. Such presentations described the applications ' security and privacy concerns. In addition, key approaches for such applications have been discussed extensively and notable privacy and security requirements have also been identified for the impaired.

Furthermore, IoT development recommendations have been published by Porambage et al. [11]. The recommendations proposed apply explicitly to education, smart homes, public safety and supply management to tackle privacy issues and concerns for different sectors. Moreover, the recommendations produced are focused on analysing the related pieces of technology or application-specific data security mechanisms and characteristics of the IoT network including the technical aspects and legislative regulations. While implementing an IoT privacy system, it offers nine features to be included.

5 Research Outputs and Proposed Solution

The outputs of a various framework elements could be linked to both the goals and research questions the above research study seeks to resolve (see Sect. 2.1). More precisely, with respect to the first research question, this was addressed with a review of the literature (RQ1) on both the key characteristics and criteria of an IoT device. For (RQ2) the findings of the research study are used to define the appropriate elements of the language of modelling. The language definition will be based on current techniques and frameworks for the network security. This will be done to make it easier for security engineering experts to use the language. The purpose for that is to allow current tooling and workflows to use Framework models, software, and processes.

The proposed contribution will be the theoretical approach and implementation of Internet of Things Privacy Policy Framework. This study also contributes to the increasing demand for field studies in the field of privacy. The obtained insights into developer approach for generating and analysing privacy standards could provide the privacy field with useful information. The privacy compliance product could not be incorporating with privacy techniques It also requires analysing the problem from its root which in some cases might be in the development phase. Maintaining IoT system's security and privacy is a complex task; the lack of open models from many frameworks and approaches is an important issue throughout the review of the literature and the implementation of the methodology. Although a number of frameworks and methods have been classified, the majority have no examples of models or the analysis other than the one incorporated in their publication.

This motivates the research project to contribute to the area of Internet of Things with a conceptual model for IoT, a methodology to construct privacy requirements and an extension in a security requirements framework that will incorporate privacy to reason IoT. The core aim of the project is to model requirement engineering privacy concepts relate to IoT throughout a conceptual

model. To achieve the above existing model of Requirements Engineering as well as models of IoT systems will be reused. The project will contribute by incorporate and extending these models and enrich them with privacy concepts required in IoT.

The novelty of contribution of the theoretical framework and the supporting tool will incorporated with the following characteristics:

- **An Internet of Things modelling language which includes conceptual model:** a conceptual model will be designed to generate privacy requirements and privacy controls whenever the required data is received.
- **Privacy for Internet of Things native devices:** there is a huge growth in the Internet of Things as different devices connect to the IoT infrastructure. Currently privacy framework focus to secure specific applications or networks. Even large corporations privacy frameworks are only considering a specific range of devices. With Internet of Things these framework are limited, since IoT network could be populated by any type of device which also includes constraint devices such as sensors and actuators.
- **Support Privacy Analysis during development and deployment:** privacy mechanisms must be used while designing a device, and then modified as it moves to different stages of development, in order to be effective. When a product have already been released the assistance is limited. When a product is launched, has to be investigated by privacy analysts to identify the vulnerabilities. Based on the type of item there may be massively different methods of monitoring. The suggested privacy framework would be able to execute on both phases, development stage, as well as stage of deployment.

6 Conclusion and Future Directions

In this work, the steps towards the development of a privacy framework for design and analysis of IoT systems along with the intermediate findings of the project research are presented. In a preliminary way, RQ1 and RQ2 are addressed with a literature review and individuation of the necessary concepts for a privacy policy language for IoT. On the basis of the results extracted from the preliminary evaluation the design of a theoretical framework which includes a language, a model for privacy policy compliance analysis and supporting tool, is currently under development. The framework consists of various components that when applied can model an Internet of Things environment which comply with privacy requirements. The main components of such framework are the modelling language to illustrate IoT environments, modelling methodology to produce models, processes to check the model's privacy and finally to present methods to extend the privacy posture of the models. The design of the framework along with the supporting tool will be as dynamic as possible. Currently existing privacy frameworks are lacking the dynamic feature as their update cycle can be span to several years which is consider quite static. The practical implementation and the validity of the framework will be examined after its completion. The validity of the artefact will be determined by a variety of case studies [12] that will use the framework in order to mitigate privacy issues.

References

1. Voas, J.: Demystifying the Internet of Things. Computer **49**, 80–83 (2016). https://doi.org/10.1109/mc.2016.162
2. Madakam, S., Ramaswamy, R., Tripathi, S.: Internet of Things (IoT): a literature review. J. Compu. Commun. **03**, 164–173 (2015). https://doi.org/10.4236/jcc.2015.35021
3. Roy, S., Manoj, B.S.: IoT enablers and their security and privacy issues. In: Mavromoustakis, C.X., Mastorakis, G., Batalla, J.M. (eds.) Internet of Things (IoT) in 5G Mobile Technologies. MOST, vol. 8, pp. 449–482. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-30913-2_19
4. Elyasaf, A., Marron, A., Sturm, A., Weiss, G.: A context-based behavioral language for IoT. In: MODELS Workshops, pp. 485–494 (2018)
5. Kammüller, F., Augusto, J.C., Jones, S.: Security and privacy requirements engineering for human centric IoT systems using eFRIEND and Isabelle. In: 2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA), pp. 401–406. IEEE, June 2017
6. Aivaloglou, E., Gritzalis, S., Skianis, C.: NETp1-08: requirements and challenges in the design of privacy-aware sensor networks. In: IEEE Globecom 2006, pp. 1–5 (2006)
7. McGraw, D.: Comprehensive privacy and security: critical for health information technology. White paper, May 2008 (2008)
8. Goldstein, M.M.: Health information privacy and health information technology in the US correctional setting. Am. J. Public Health **104**(5), 803–809 (2014)
9. Alqassem, I., Svetinovic, D.: A taxonomy of security and privacy requirements for the Internet of Things (IoT). In: 2014 IEEE International Conference on Industrial Engineering and Engineering Management, Bandar Sunway, pp. 1244–1248 (2014)
10. AL-mawee, W.: Privacy and security issues in IoT healthcare applications for the disabled users a survey (2012)
11. Porambage, P., Ylianttila, M., Schmitt, C., Kumar, P., Gurtov, A., Vasilakos, A.V.: The quest for privacy in the Internet of Things (2016)
12. Piras, L., et al.: Defend architecture: a privacy by design platform for GDPR compliance. In: 16th International Conference on Trust, Privacy and Security in Digital Business (TrustBus) (2019)
13. Al Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of Things: a survey on enabling technologies, protocols, and applications (2015)
14. Atzori, L., Iera, A., Morabito, G.: The Internet of Things: a survey (2010)
15. Mahmoud, R., Yousuf, T., Aloul, F., Zualkernan, I.: Internet of Things (IoT) security: current status, challenges and prospective measures, Vancouver (2010)
16. Madhura, P.M., Jain, P., Ranjith, J., Bilurkar, N.: A survey on internet of things: security and privacy issues. IJITR **3**(3), 2069–2074 (2015)
17. Wieringa, R.J.: Design Science Methodology for Information Systems and Software Engineering. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-43839-8
18. March, S.T., Storey, V.C.: Design science in the information systems discipline: an introduction to the special issue on design science research. MIS Q. **32**(4), 725–730 (2008)