Privacy Representation in the Internet of Things Using Pretopological Theory

Amri Toumia
University Paris VIII
Saint-Denis, France
amri.toumia@etud.univ-paris8.fr

ABSTRACT

Data security and privacy protection have been identified as one of the most critical issues of the Internet of Things (IoT). They represent one of the major obstacles to its adoption. Researchers have addressed the matter by extensive work on protection algorithms and mechanisms. However, setting up privacy preferences is still a complicated task for users. Understanding their impact on personal data is also hard to grasp for non-technical users. Continuing our previous work, we present in this article a first implementation of our precedent model and how to use it for a representation that allows users to configure their privacy preferences graphically.

CCS CONCEPTS

• **Security and privacy** → **Privacy protections**; • **Computing methodologies** → *Model development and analysis*; • **Hardware** → *Sensor devices and platforms*;

KEYWORDS

Privacy, Internet of Things, Modeling, Pretopology

ACM Reference Format:
Amri Toumia. 2018. Privacy Representation in the Internet of Things Using Pretopological Theory. In *Digital Tools & Uses Congress (DTUC '18), October 3–5, 2018, Paris, France.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3240117.3240134

1 INTRODUCTION

With the Internet of Things (IoT), smart devices will be generating a huge amount of data about people and their surroundings. This information is usually sent to servers where they are stored, processed and analyzed to be used to help in decision-making.

In this context, privacy must be ensured within connected devices, during the transmission, storage and processing of information. Indeed, data security and privacy protection have been identified as one of the most critical issues of IoT, and represent one of the major obstacles to its adoption.

To solve this problem, many scientists have addressed the issue. A lot of work on data protection and privacy in IoT can be found in the literature.

DTUC '18, October 3–5, 2018, Paris, France

ACM ISBN 978-1-4503-6451-5/18/10…$15.00
https://doi.org/10.1145/3240117.3240134

Despite that, configuring privacy protection is still a complicated task for users and understanding the impact of a set of privacy preferences on personal data is hard to grasp for non-technical users.

The objectives of this paper are to study privacy protection in the IoT and its configuration according to the preferences of the users. Through pretopology, can we create a graphic and conceptual organization of privacy and allow its setting by manipulating the graphical elements of a diagram?

In a previous work[20], after presenting pretopological theory and assessing the state of the art in privacy protection, we studied the benefits of using pretopology concepts for modeling data sharing and thus representing privacy. We showed that the pseudoclosure operator helps track the propagation of an information and the actors involved in the process. We took as a case study a smart-watch that can collect information about the user, such as heart rate, blood pressure, localization and body temperature.

In our representation, we consider a set E composed with memory spaces of devices and actors of the digital world. In the context of privacy, it is interesting to study the propagation of information from one memory space to another. Thus, for our case study, we showed how we could represent data sharing between actors in the IoT environment.

This approach conveniently provides a general framework that allows us to model and represent the connections between memory spaces. So, it becomes easier to see how data is propagated from one entity to another and who can access a certain information.

After the introduction, the paper continues with presenting important work in the literature that deals with privacy protection in the IoT. Then, we will study how to model privacy preferences in IoT using pretopology and we will show the first results of the implementation of this model using the pretopolib library. Finally, we discuss our results and provide recommendations for future work. In addition, in the appendix, we define pretopology and list its concepts.

2 IOT AND PRIVACY PROTECTION

The Internet of Things is a new concept that refers to interconnected devices, systems, and services that rely on autonomous communication between physical objects within the existing Internet infrastructure. This makes it possible to bring the knowledge of the Internet to physical objects, making them capable of communicating and exchanging data in the context of different fields of applications, such as, for example, health, environment, transport , industry and recreation [12]. The development of the IoT brings a redefinition of the digital frontiers [4] which strongly impacts our

societies on the technical, industrial, economic, social and political [18], [16].

In the IoT, the environment is measured and analyzed using sensors and connected devices. The collected information is then sent to a server that contains the business logic. In this context, privacy must be ensured within connected devices, during the storage, transmission and processing of information [1]. Indeed, data security and privacy protection have been identified as one of the major issues of IoT, and represent one of the major obstacles to its adoption [3].

To solve this problem, many scientists have addressed the issue. A lot of work on data protection and privacy in IoT can be found in the literature. The solutions proposed concern the protection of data transmitted to the cloud [11] [7] [14].

Other authors have focused on data protection by cryptographic mechanisms adapted to an IoT environment characterized by low computing power. Among them, we can cite the work of [17] [8] and [15].

In addition, there is also other work that focuses on protecting the privacy of users in IoT by defining privacy policies and protection preferences. Davies et al. [6] have developed what they call a "privacy mediator". Based on cloudlet technology, their system consists of a module that is inserted into the data distribution pipeline. It aggregates and obfuscates data and helps enforce privacy policies in place before data is released from the user's control to be sent to the cloud.

Also, Neisse et al. have proposed SecKit [13], a framework applied to the case of a smart city, especially the interactions between a smart home, a smart vehicle and a smart office. The main part of the proposed solution is a control tool, where privacy policies can be used to regulate access to data and resources in IoT, with the ability to support the dynamic change of context.

Finally, Chen et al. have developed CoBrA (Context Broker Architecture) [5], a framework that takes into account the security and privacy aspect of IoT. It is used for the smart meeting room case, where the confidentiality of the data exchanged there and the protection of the privacy of the participants is a priority. Their article also highlights the challenge of protecting privacy when the context changes dynamically and users must manually set their privacy policies for each context.

We note that, when dealing with setting privacy preferences in the IoT, users often find themselves lost in the face of the complexity of the system and fail to conceive the repercussions of sharing information about their private lives. In this context, pretopology can be a practical tool to enable users to define their privacy preferences and better control information sharing through visual tools.

3 PRETOPOLOGY AND PRIVACY PROTECTION IN IOT

In this section, we will study how to model privacy preferences in IoT using pretopology. For this, we use a smart watch as an example of a smart device. This watch can measure the blood pressure (BP), the heart rate (HR), the temperature (T), and location (L) of a user.

Let us consider a set E consisting of the memory spaces of the devices and actors of the digital world. Subsets of this set can be constituted by the storage spaces of those devices and actors. In the case of privacy protection, it would be interesting to study the diffusion of information from one memory space to another. Thus, the pseudoclosure function could be that which associates the memory space of one entity to another following the diffusion (or copying) of a given piece of information.

Consider a first example where the user shares information about his BP and HR with an IoT Platform that provides various services in relation with his device. As described earlier, the pseudoclosure process represents the sharing of information from one memory space to another.

We have, then, $M = (BP, HR, T, L)$ representing the measures done by the smart watch and saved on its memory space. The pseudoclosure of M, $a(M)$ means storing BP and HR of the smart watch in the memory space of the IoT Platform. So:

$$a(M) = (BP, HR, T, L, BP_1, HR_1) \quad \begin{array}{l}\text{with } \mathrm{BP}_1 \text{ and } \mathrm{HR}_1 \text{ the}\\ \text{memory spaces of the IoT}\\ \text{Platform which will hold}\\ \text{BP and HR of the user}\end{array} \tag{1}$$

The interior of M is :

$$i(M) = C.a.C(M) = C.a(E - M) = M \tag{2}$$

As for the exterior of M, it is as follows :

$$ex(M) = C.a(M) = E - a(M) \tag{3}$$

The edge of the subset M is :

$$ed(M) = M \cap a.c(M) = M \cap a(E - M))M\ cap(E - M) = \emptyset \tag{4}$$

The surround of M is :

$$surr(M) = a(M) \cap C(M) = (BP_1, HR_1) \tag{5}$$

Finally, the frontier of M :

$$\delta(M) = ed(M) \cup surr(M) = (BP_1, HR_1) \tag{6}$$

Using an adaptation of the library pretopolib [9], and entering information about the pseudoclosure process, we were able to calculate the interior, the edge, the surround and the exterior of M. We then used them to construct a json that we used with D3.js and obtained the following representation (Fig 1)

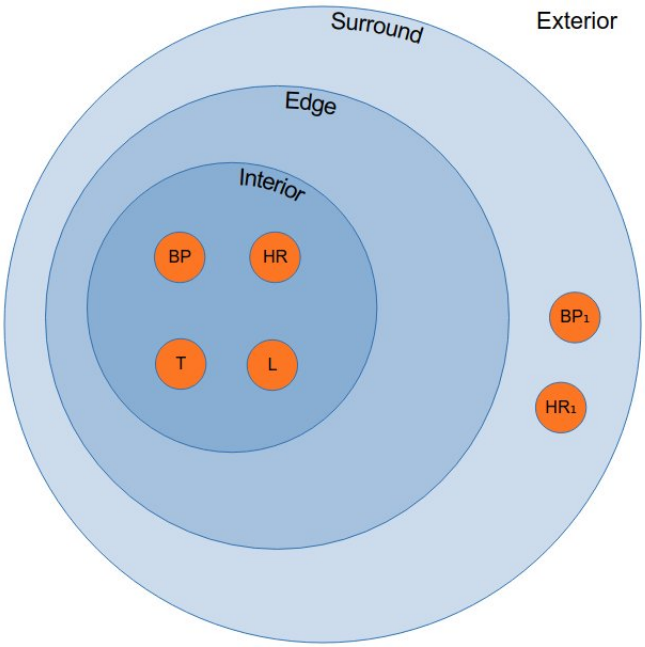

Figure 1: Topological representation of information sharing with IoT Platform

Through this graphic representation of privacy preferences, the user can see which data are shared with the IoT platform. We can also see that shared data (BP_1 and HR_1) do not belong only to the user but also to the platform, where they are saved on its memory space.

Configuring what to share can be realized directly via the graphic. By moving the orange circles from a subset to another, users can reconfigure their privacy preferences.

Suppose now that the platform with which the user shared his data shares them in turn with a third party. The latter can be an advertiser who, thanks to the location data, will propose more targeted content or an insurance that could adapt its prices according to the way of life of the users. Of course, according to the new privacy laws, the platform is obliged to inform the user of the transmission of its data to a third party and also has the duty to specify the purpose of their collection.

We will have, as we have described above, a process of expansion of M because of the successive application of adhesion, or, in other words, because of the transmission of information from one actor to another . The transmission of user data to the third party via the IoT platform can be modeled in pretopology as follows:

$$\begin{aligned} a^2(M) &= a(a(M)) \\ &= a((BP, HR, T, L, BP_1, HR_1)) \\ &= (BP, HR, T, L, BP_1, HR_1, BP_2, HR_2) \end{aligned} \tag{7}$$

Same as before, we obtained the following representation (Fig 2)

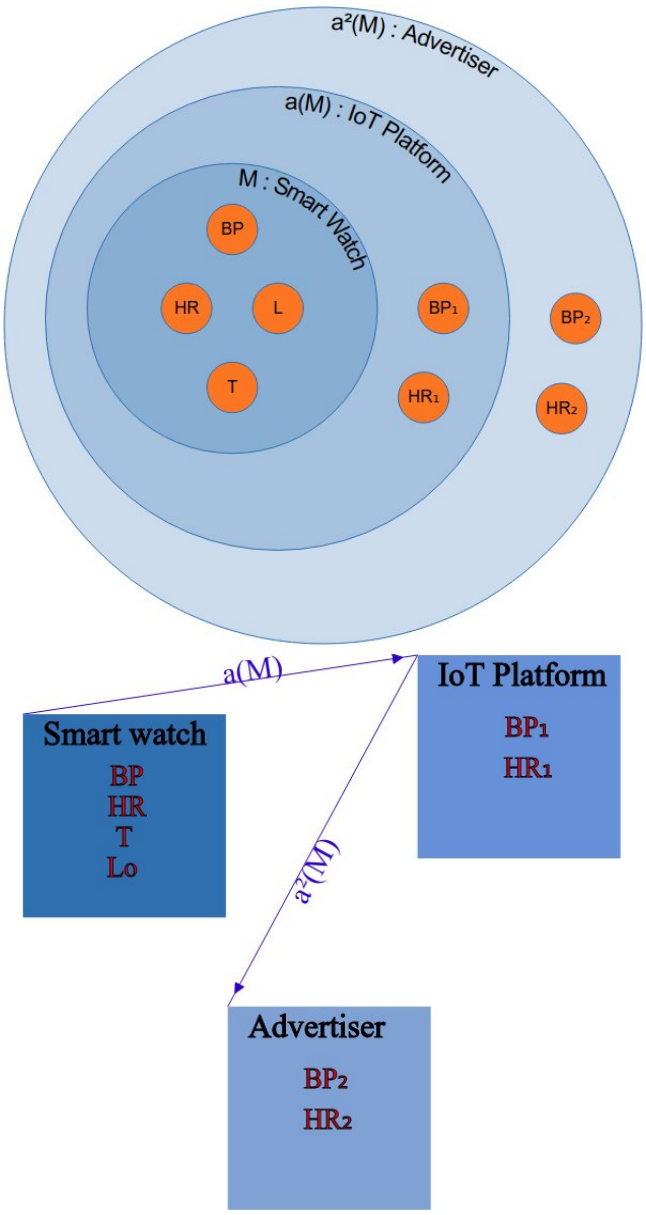

Figure 2: Dilation of M

Through this representation, it is easier to understand how the data is passed from one entity to another. Also, users have the possibility to stop sharing some information just by clicking on its corresponding circle and deleting it. Moreover, it is possible to share more data with an entity by dragging the corresponding circle in it. All these actions will result in recalculating the topological representation of information sharing and reconfigure the privacy settings.

4 CONCLUSION AND FUTURE WORK

We have exposed in this paper what pretopology could bring to the modeling of privacy. We have seen that thanks to the concept

of pseudoclosure, we can model the sharing of information or the authorization to access it. Thanks to its definition of the concept of proximity, pretopology allows us to have a graphic representation of information sharing. This representation was the basis of a visual system of parameterization of the privacy. Thanks to the latter, the user will define his preferences more easily and will have a better idea of the impact of his choices on access to his personal data.

In our future work, we will deepen our study on the representation of data transmission in IoT and improve our model implementation. We will also seek to analyze the privacy policies of some IoT platforms to identify what they collect as information and for what purposes, as well as to which other entities they transmit it in order to achieve a more detailed modeling. We hope that from this, the user will be able to configure their privacy preferences more easily and will be more aware of the impact of sharing this data with an entity.

A DEFINITION OF PRETOPOLOGY

Pretopology results mainly from the work of a group of researchers called Z. Belmandt [2], which sought to reduce the axiomatic complexity of general topology. In the same way as topology, pretopology deals with questions of proximity and neighborhood, without bringing these notions back to the use of a distance. Indeed, the operator who structures the pretopology is not the distance, but an elementary operator while being general which associates with a part its extension.

B PRETOPOLOGICAL CONCEPTS

In this section, we will recall some of the basic pretopological concepts from the article [10] :

B.1 Pseudoclosure

A map $a(.)$ from $P(E)$ to $P(E)$ is called a *pseudoclosure* if and only if $\forall A \in P(E)$:

(1) $a(\emptyset) = \emptyset$
(2) $A \subset a(A)$

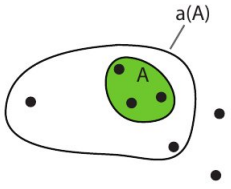

Figure 3: Pseudoclosure of a set A [10]

B.2 Interior

Let $a(.)$ be a pseudoclosure on E, the map interior $i(.)$ is :

$$\forall B \in P(E), i(B) = C.a.C(B) \tag{8}$$

where $C(B)$ is the complement of the set B
The interior verifies :

(1) $i(E) = E$
(2) $\forall B \subset E, i(B) = B$

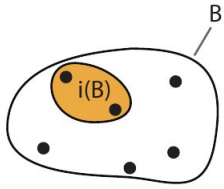

Figure 4: Interior of a set B [10]

B.3 Near, Far, Intermediate

In pretopology, the exterior of a set is defined by the complement of its pseudoclosure :

$$\forall A \in P(E), ex(A) = C.a(A) \tag{9}$$

The exterior is composed of elements that can be considered as far from the set. In contrast to the interior, where the elements in it are considered close to each other. [19]

Between the interior and the exterior lays the border which is composed of two parts : the edge and the surround [19] :

$$\forall A \in P(E), ed(A) = A \cap a.C(A) \tag{10}$$

$$\forall A \in P(E), surr(A) = a(A) \cap C(A) \tag{11}$$

$$\forall A \in P(E), \delta(A) = ed(A) \cup surr(A) \tag{12}$$

B.4 Pretopological Space

The triplet (E, i, a) is called a pretopological space.
The most interesting spaces are those of the type V. They have the following property:

$$\forall A \in P(E), B \in P(E), A \subseteq B \Rightarrow a(A) \subseteq a(B) \tag{13}$$

B.5 Open and Closed Subsets

In V type pretopological spaces, the dilation process (cf. Fig. 5) caused by the pseudoclosure map stops at a given moment and no longer evolves. In that case, we have:

$$\forall A \in P(E), a^{k+1}(A) = a^k, \text{with k} \in \mathbb{N} \tag{14}$$

A is then called a closed subset.
In the same way, the evolution of the interior will cease, which gives:

$$\forall A \in P(E), i^{k+1}(A) = i^k \tag{15}$$

A is then called an open subset.

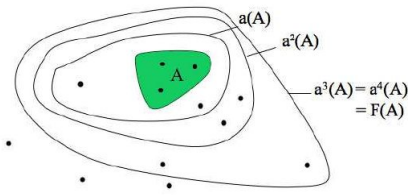

Figure 5: Successive pseudoclosure of A leading to a closed subset [10]

REFERENCES

[1] Amira Barki, Abdelmadjid Bouabdallah, Said Gharout, and Jacques Traore. 2016. M2M Security: Challenges and Solutions. *IEEE Communications Surveys & Tutorials* 18, 2 (2016), 1241–1254. https://doi.org/10.1109/COMST.2016.2515516

[2] Z Belmandt. 1993. Manuel de prétopologie et ses applications: sciences humaines et sociales, réseaux, jeux... (1993).

[3] Elisa Bertino. 2016. Data Security and Privacy in the IoT. *Proceedings of the 19th International Conference on Extending Database Technology* (2016), 1–3. https://doi.org/10.5441/002/edbt.2016.02

[4] Naserddine Bouhaï, Imad Saleh, and Hakim Hachour. 2016. *Frontières numériques et artéfacts.* Editions L'Harmattan.

[5] H. Chen, T. Finin, Anupam Joshi, L. Kagal, F. Perich, and Dipanjan Chakraborty. 2004. Intelligent agents meet the semantic Web in smart spaces. *IEEE Internet Computing* 8, 6 (nov 2004), 69–79. https://doi.org/10.1109/MIC.2004.66

[6] Nigel Davies, Nina Taft, Mahadev Satyanarayanan, Sarah Clinch, and Brandon Amos. 2016. Privacy Mediators : Helping IoT Cross the Chasm. *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications - HotMobile '16* (2016), 39–44. https://doi.org/10.1145/2873587:2873600

[7] Martin Henze, Sebastian Bereda, René Hummen, and Klaus Wehrle. 2014. SCSlib: Transparently Accessing Protected Sensor Data in the Cloud. *Procedia Computer Science* 37 (jan 2014), 370–375. https://doi.org/10.1016/J.PROCS.2014.08.055

[8] Reshma Kotamsetty and Manimaran Govindarasu. 2016. Adaptive Latency-Aware Query Processing on Encrypted Data for the Internet of Things. In *2016 25th International Conference on Computer Communication and Networks (ICCCN).* IEEE, 1–7. https://doi.org/10.1109/ICCCN.2016.7568488

[9] Vincent Levorato. 2010. *Contribution a la Modélisation des Réseaux Complexes : Prétopologie et Applications.* Ph.D. Dissertation. https://tel.archives-ouvertes.fr/tel-00460708

[10] Vincent Levorato. 2010. Une méthode mixte d'analyse d'un réseau social: classification prétopologique et centralité d'intermédiarité. (2010), 5–77. https://hal.archives-ouvertes.fr/hal-00460637/document

[11] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou. 2013. Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. *IEEE Transactions on Parallel and Distributed Systems* 24, 1 (jan 2013), 131–143. https://doi.org/10.1109/TPDS.2012.97

[12] Shancang Li, Li Da Xu, and Shanshan Zhao. 2015. The internet of things: a survey. *Information Systems Frontiers* 17, 2 (2015), 243–259. https://doi.org/10.1007/s10796-014-9492-7 arXiv:arXiv:1011.1669v3

[13] Ricardo Neisse, Gary Steri, Igor Nai Fovino, and Gianmarco Baldini. 2015. SecKit: A Model-based Security Toolkit for the Internet of Things. *Computers & Security* 54 (2015), 60–76.

[14] B. Pooja, M. M. Manohara Pai, and M. Pai Radhika. 2014. A Dual Cloud Based Secure Environmental Parameter Monitoring System: A WSN Approach. Springer, Cham, 189–198. https://doi.org/10.1007/978-3-319-05506-0_18

[15] Sanaah Al Salami, Joonsang Baek, Khaled Salah, and Ernesto Damiani. 2016. Lightweight Encryption for Smart Home. In *2016 11th International Conference on Availability, Reliability and Security (ARES).* IEEE, 382–388. https://doi.org/10.1109/ARES.2016.40

[16] Imad Saleh. 2017. Les enjeux et les défis de l'Internet des Objets (IdO). *Internet des objets* 1, 1 (2017).

[17] Hossein Shafagh, Anwar Hithnawi, Andreas Droescher, Simon Duquennoy, and Wen Hu. 2015. Towards Encrypted Query Processing for the Internet of Things. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking - MobiCom '15.* ACM Press, New York, New York, USA, 251–253. https://doi.org/10.1145/2789168.2795172

[18] Samuel Szoniecky and Stéphane Safin. 2017. Modélisation éthique de l'Internet des Objets. *Internet des objets* 17, 2 (jun 2017). https://doi.org/10.21494/ISTE.OP.2017.0148

[19] Serge Thibault. 2017. Prétopologie et espaces habités. *EspacesTemps. net* (2017).

[20] Amri Toumia and Samuel Szoniecky. 2018. Prétopologie et protection de la vie privée dans l'Internet des Objets. *Open Science-Internet des objets* 2, 1 (2018).