Internet of Things Context-Aware Privacy Architecture
Selt Rachid, Yacine Challal, Benblidia Nadjia

▶ To cite this version:

HAL Id: hal-01308839
https://hal.archives-ouvertes.fr/hal-01308839
Submitted on 28 Apr 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Internet of Things Context-Aware Privacy Architecture

Selt Rachid1, Yacine Challal2,3, Benblidia Nadjia1

1Research Laboratory for the Development of Computerized Systems (LRDSI), University Saad Dahleb of Blida (USDB), Blida, Algeria
2Ecole nationale Supérieure d’Informatique (ESI), Laboratoire LMCS, Algeria
3Sorbonne Universités, Université de Technologie de Compiègne Laboratoire Heudiasyc, UMR CNRS 7253, France

Abstract—

The Internet of Things (IoT) is a rapidly growing technology in recent years. It represents an extension of the Internet into the physical world embracing everyday objects. In consequence, users’ privacy and security are becoming a great challenge. To cope with this issue, sophisticated approaches are needed to guarantee these services and hence ensure a large-scale adoption of IoT. In our work we present an approach to model and describe the architecture of internet of things, in which user privacy and security are ensured while taking into consideration the dynamic context in which evolve users, their experience and preferences with respect to security and privacy.

Keywords—Internet of things; privacy; security; context-aware; architecture

I. INTRODUCTION

Internet of Things definition is given by [1]: “things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts”.

In recent years, user data privacy and security pose a great challenge in the context of Internet of things. Indeed, if all our devices are connected to the Internet we can be sure that they will be of great interest to various criminals who wish to monitor us. For this reason the privacy and security of IoT is becoming a hot research topic.

In this article, we propose a context-aware architecture for privacy preservation in IoT. We introduce the three layers of our architecture and main components.

The remainder of this paper is organized as follows, in section II we present related works. We present our context-aware privacy architecture for IoT and use cases in Section III. Conclusion is given in section IV.

II. RELATED WORKS

Schmidt et al. [8] proposed a context data model for context data stemming from the user himself and his surroundings. In [7], authors proposed a privacy-aware solution where the privacy value denotes how much the user is willing to share the related information with other actors in the system. In [6] Huang et al. proposed a context-aware model to ensure the privacy of users, without taking into consideration the user data augmentation and the inference mechanism. In [3], Pietschmann et al. proposed ontology-based context management service; they don’t represent the privacy of users and the security in their ontology.

All of these works deal with privacy problem and/or security for IoT. Although they propose models or architectures, they do not take into consideration the user context and security policy adaptation with respect to user’s context evolution. We will show that our solution outperforms existing solutions thanks to providing security policy adaptation that relies on an inference engine. We will provide details regarding our architecture in the following section.

III. CONTEXT-AWARE PRIVACY ARCHITECTURE FOR IoT

A. Architecture Security Levels

In IoT there are different levels of security: the security of devices, communications and users.

1) Security of devices

At this level, security deals with the protection of hardware and the software run by devices (operating system and applications).

2) Security of communication

Network security is a great challenge: technologies like RFID, NFC, and WSN must have a secure data communication to save the data transmitted between objects and assure that no third entity not authorized can stole the information.

3) Security of users

In this level the user privacy and security should be protected: the user information like health condition or position must be kept private and accessible only for the authorized entities.

In our architecture Fig 1 we based on the architectural model for IoT presented in [2], that is composed of three layers 1) sensing layer; 2) network layer; 3) application layer
The distributed privacy protection systems in our architecture use an ontology that describes the privacy of users. This ontology fulfills the various requirements. First of all, it serves as a common vocabulary for representing the context shared across the various system components. It also serves as an intuitive way to describe complex privacy requirements that connect various private data types with different types of services and associate access to this data with policies.

2) Ontology as a service

The ontology of privacy rules is saved in the cloud. It is accessible as a service to give the possibility to access it from any place, any device and any time. Knowledge representation by ontology may be accompanied with reasoning mechanisms and inference algorithm. The reasoning mechanisms allow us to request the ontology and extract the knowledge we need, however the inference algorithm is to produce new security rules based on the old ones.

There are two possibilities to apply the inference rules; at each event or request information from ontology, or each time interval.

IV .CONCLUSION

In this paper we presented a SOA architecture for context-aware privacy and access control in the Internet of things. Our architecture aims to protect users’ privacy and provide access control while taking into consideration users’ context and security requirement. Our solution relies on an ontology to describe both users’ context and access policies.

This architecture allows users to control sharing and using their information in the context of the Internet of things, and with the inference in the ontology we can produce new rules based on the initial rules to support context-evolution.

REFERENCES

[5] Xin Huang, Rong Fu, Bangdao Chen, Tingting Zhang, and A. W. Roscoe * User Interactive Internet of Things Privacy Preserved Access Control * Third International Conference on Communication Theory, Reliability, and Quality of Service 2012.