Bubbles of Trust: a decentralized Blockchain-based authentication system for IoT

Mohamed Tahar Hammi, Badis Hammi, Patrick Bellot, Ahmed Serhrouchni

PII: S0167-4048(18)30089-0
DOI: 10.1016/j.cose.2018.06.004
Reference: COSE 1357

To appear in: *Computers & Security*

Received date: 14 February 2018
Revised date: 8 June 2018
Accepted date: 20 June 2018

Please cite this article as: Mohamed Tahar Hammi, Badis Hammi, Patrick Bellot, Ahmed Serhrouchni, Bubbles of Trust: a decentralized Blockchain-based authentication system for IoT, *Computers & Security* (2018), doi: 10.1016/j.cose.2018.06.004

Bubbles of Trust: a decentralized Blockchain-based authentication system for IoT

Mohamed Tahar HAMMI*†, Badis HAMMI*, Patrick BELLOT*† and Ahmed SERHROUCHNI*†
*LTCI, Telecom Paristech, France
† Paris Saclay University, France
hammi, bhammi, bellot, serhrouchni@telecom-paristech.fr

***Abstract*—There is no doubt that Internet of Things (IoT) occupy a very important role in our daily lives. Indeed, numerous objects that we use every time, are being equipped with electronic devices and protocol suites in order to make them interconnected and connected to the Internet. In IoT, things process and exchange data without human intervention. Therefore, because of this full autonomy, these entities need to recognize and authenticate each other as well as to ensure the integrity of their exchanged data. Otherwise, they will be the target of malicious users and malicious use. Due to the size and other features of IoT, it is almost impossible to create an efficient centralized authentication system. To remedy this limit, in this paper, we propose an original decentralized system called *bubbles of trust*, which ensures a robust identification and authentication of devices. Furthermore, it protects the data integrity and availability. To achieve such a goal, our approach relies on the security advantages provided by blockchains, and serves to create secure virtual zones (*bubbles*) where things can identify and trust each other. We also provided a real implementation[1] of our mechanism using the *C++* language and *Ethereum* blockchain. The obtained results prove its ability to satisfy IoT security requirements, its efficiency, and its low cost.**

***Index Terms*—IoT, Security, Authentication, Blockchain, Smart city, Ethereum**

I. Introduction and problem statement

Currently, over the world, Internet of Things (IoT) is involved in almost all the fields of our daily life. According to a recent *Gartner* study, 50 billion connected devices[2] will be deployed by 2020 [1]. Indeed, citizens are gradually equipping their homes with IoT devices such as smart TVs, Internet boxes, heating systems, home's remote control, lighting systems and so on. In factories and industrial environments, the cooperation of robots and other smart tools enhances the efficiency of automation systems and allows better productions. The IoT involvement did not stopped to these use cases, but, is widely adopted in many other areas such as health care, military, agriculture and smart cities.

IoT represents the principal actor to make our cities smarter. This fact was extensively addressed during the last *United Nations conference on climate change (Cop21)* held in Paris in 2016. It was concluded that connected objects have the potential to considerably reduce CO_2 emissions[3]. Besides, IoT can bring other vital applications in the context of smart cities, such as: intelligent waste management, buildings' health, environmental monitoring, intelligent transportation systems, smart parking, traffic management, smart navigation system for urban common transport riders, smart grid, and multiple other applications [2].

Besides, IoT allowed the evolution of many other areas such as: (1) factories to what is actually called industry 4.0 [3], (2) agriculture to smart agriculture [4] [5], (3) health to smart health [6] [7] and many other examples.

The idea behind IoT and its different applications, is the omnipresence of a variety of things, where they are able to interact and cooperate with each other in order to provide a wide range of services. Thus, a huge number of devices will be included. Each physical or virtual device should be reachable and produce content that can be retrieved by users regardless of their location [8]. However, It is very important that only authenticated and authorized users make use of the system. Otherwise, it will be prone to numerous security risks such as information theft, data alteration and identity usurpation. Indeed, security issues remain the major obstacle to the large scale adoption and deployment of IoT since it is highly vulnerable to attacks for numerous reasons: (1) most of the communications are wireless, which makes the system more vulnerable to numerous attacks such as identity spoofing, messages eavesdropping, messages tampering and other security issues, and (2) multiple types of devices have limited resources in terms of energy, memory and processing capacity, which prevent them from implementing advanced security solutions.

Many researchers [9] [10] qualify IoT as a system-of-systems, where, multiple use case scenarios require that only trusted users can use offered services. Thus, conventional security requirements such as authentication, confidentiality, and data integrity are critical to each part of these ecosystems, including things, networks, and software applications. However, due to limitations and heterogeneity of devices' resources, existing security solutions are not fully adapted to such an ecosystem. Besides, often, the combination of multiple security technologies and solutions is needed, which leads

[1] A video that shows the realized implementation, development and functioning of the approach is available on: https://www.youtube.com/watch?v=XE13QGR1czE&t=169s.

[2] In the remaining of this paper, we use indifferently the terms device, thing, object and smart thing in order to refer to a connected smart thing.

[3] http://blogs.gartner.com/smarterwithgartner/cop21-can-the-internet-of-things-improve-organizations-sustainability-performance/.