Future Generation Computer Systems 74 (2017) 444–466

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Midgar: Study of communications security among Smart Objects using a platform of heterogeneous devices for the Internet of Things

Gonzalo Sánchez-Arias *, Cristian González García, B. Cristina Pelayo G-Bustelo

University of Oviedo, Department of Computer Science, Sciences Building, C/Calvo Sotelo s/n 33007, Oviedo, Asturias, Spain

HIGHLIGHTS

- Security in an insecure IoT environment.
- Securing user privacy in the messages through a IoT network.
- Using cryptography to create secure messages in IoT.
- Comparison of different cryptographic algorithms.
- Implementation of one possible cryptography solution in based on the performance.

ARTICLE INFO

Article history:
Received 30 June 2016
Received in revised form
9 January 2017
Accepted 28 January 2017
Available online 2 February 2017

Keywords:
Internet of Things
Privacy
Security
Cryptography
Ubiquitous computing
Smart Objects
Communications

ABSTRACT

In last years, the Internet of Things has been a revolution in terms of applications and research. Currently, there are a great variety of nodes connected to each other to create different applications in areas, ranging from sport to business, inter alia. These applications compromise our private information about our bank accounts, health, and location. This makes us take safety measures to achieve a secure communication, where the interception of a message by a malicious user cannot compromise our privacy.

This security encompasses a very broad concept that can be addressed in multiple ways. This work focuses on the techniques and cryptographic algorithms that can be used in the messages exchanged among the nodes to create secure Internet of Things networks in a way to protect our communications. In this article, we have used the Midgar platform to evaluate the different possibilities of traditional security techniques related to cryptography with the purpose of testing the different combinations to find a solution for the Internet of Things when it uses insecure protocols. Analysing the results to determine the best solution, in terms of costs and security, we concluded that the use the RSA, AES and SHA-3 algorithms are a real possibility to protect message privacy among smart objects. This combination offers the lowest consumption–security relation among all the combinations that we have tested in our evaluation.

1. Introduction

Nowadays, we can find a myriad of applications which benefiting from the available technology to make our daily lives easier [1,2], but only represent a little sample of all the different applications that could be applied in our everyday life in the future [2,3]. These applications are the result of the boom in Smart Objects [4] and the great range of possibilities they offer that allow us to monitor data as personal information or information from our surroundings and act consequently or responding automatically. These possibilities exist due to the different sensors incorporated in our smartphones [5] and tablets [6], in addition to other technologies which appear or evolve in parallel with this revolution. I.e.: the use of smartphones [7], intelligent tags [8,9] or the new SmartBands. All of these combinations are developed in the actual context of the Internet revolution, the cloud computing, and the large datasets processing through Big Data. The combination of this context and the new technologies make possible the Internet of Things (IoT) [10].

The Internet of Things allows us to keep objects scattered all over the world in order to receive information from our homes, our work, our car, or from hostile areas [11]. Or even from the bottom of the ocean [12], a similar vision to that exposed in [13] about the ignorance of where data is geographically located at any particular

* Corresponding author.
E-mail addresses: gonzalo.sanchez.arias@gmail.com (G. Sánchez-Arias), gonzalezgarciacristian@hotmail.com (C. González García), crispelayo@uniovi.es (B.C. Pelayo G-Bustelo).

http://dx.doi.org/10.1016/j.future.2017.01.033
0167-739X/

time in the cloud. Those objects can explore their surroundings, communicate with other objects or with human beings, helping them to complete their tasks in intuitive ways [1]. I.e.: the sensors placed in a particular infrastructure can offer information about the environmental conditions or detect someone trespassing a private area, and they could act accordingly [6]. Most of these sensor nodes are deployed in the unmanned environment, and due to lacking of effective protection measures, the signal exposed to the public are vulnerable to malicious attacks [14]. This will lead to a future in where it will not be used just to communicate people, but also to communicate people with machines and even machines with machines (M2M) [9,12], easing different communication patterns like user-to-user, user-to-device, device-to-device, and devices-to-user [15]. In that way, those nodes can complete general tasks as controlling a thermostat, or more personal data as collecting and reporting information about our health, our usual routes, our bank accounts or our location. This means that nodes exchange public and private information that should not be revealed. Also, users generally keep their mobile devices switched on all day, even during night-time, which means that the sensors integrated are still collecting data and the user is inadvertently revealing information about where he is and what he is doing [15].

We can see an example of personal information that can use these applications in [16], where they place SmartBands around wrists of some users while they attend as audience to the narration of a story. As the plot develops, the users have to 'enter' into the story, so they will be confronted with different situations and scenes, to which they have to react and even eventually make decisions. The SmartBands analyses the electrodermal changes of the subject's skin and after, the SmartBand sends the data about the sensations the user has experimented in the test to other objects in order to identify moods like excitement, concentration or surprise, to make a quantitative analysis. Those bracelets could be of use in many different contexts, i.e. to inform about the level of concentration of an employee while working or a student during a lecture, and maybe not everyone is willing to disclose this information. Another example is [17] where the authors develop services in the benefit of people with special needs and/or the elderly by a system of wireless communication which allows an easy contact with their caretakers and the storage of data in the cloud, which could also be used to control patients with chronic diseases [6].

As we can see, the type of the applications of this technology and the data used in them have a problem with de users' privacy. These data are very important in a new world where information from millions or even billions of users devices can be collected, processed and exploited collaboratively within a global Internet of Things network [18]. We understand privacy as the right of an individual to determine the amount of information available to other [19].

The personal character of this information endangers our intimacy and forces us to take security measures in order to secure the communications without the risk of having one of our messages intercepted by malicious users because the urge to discover secrets is deeply ingrained in human nature [20]. These security measures could be applied in different ways and, due to the novelty of the IoT, they should be checked regularly having in mind other aspects that may have been overlooked previously [21]. These vulnerabilities could be rather simple as a physical attack due to the individual or lonely character of the nodes, which can have a lack of vigilance; or more technical, using the wireless communication to spy the channel used to transfer the data [2]. That is the reason why this research work is going to focus mainly on the communication between the objects and the transmission of a secure message through an insecure channel.

To this purpose, we will look for the measures that can protect the message exchange by an IoT network nodes and prevent it from being violated by malicious users, in such way that, even though they intercept them, they will not be able to read them. This is why we have also been based on the knowledge acquired from studies on the prevention of computer attacks that do not require human interaction as [22]. The measures we will be using consist on cryptographic techniques from the traditional security to encrypt the message sent at the moment of the communication. We use the cryptography because it is necessary when communicating over any untrusted protocol, which includes just about any network, particularly the Internet [23]. Such measures have recently been included in the popular instant messaging application WhatsApp [24], by encrypting the message exchange between users.

However, the IoT cannot adopt a cryptographic technology because the cryptographic techniques need a large amount of computing [14,25] and many IoT devices are not currently powerful enough to support robust encryption [26]. The traditional security measures cannot be directly applied to IoT technologies because the high number of interconnected devices makes scalability issues [27]. This is why we will include the minimum measures to ensure the privacy protection of the data transmission in the network. First of all, the techniques will be evaluated, depending on the kind of used cryptography. Then, we will analyse different cryptographic methods like the secret or private key, the public or asymmetric key, and the hybrid cryptography. After that, we will study the algorithms that could be used on each type above-mentioned in order to establish the best possible combination. We must perform this analysis phase because these techniques were not created to be used in the IoT [28], and their process and use could present major impediments when applied to some devices.

These security measures should be relevant to the message exchange among the objects interconnected through the IoT, so they will be applied in the platform Midgar [12,29]. The Midgar platform generates applications that interconnect heterogeneous objects among themselves, facilitating the creation of these applications in an easy way for any type of people. Besides, Midgar collects information about the device sensors and makes interact among them according to the context, which was defined by the users. This is why the security cannot be never neglected in this platform, where more or less all the IoT context is represented.

The main objective of our work is to demonstrate that cryptographic measures can be taken to protect the communions in a part of the Internet of Things, in this case in the message exchange, without this entailing an excessive cost. The related works, as we can see in Section 2.8, defended the low computing capacity of the devices that have a place in these communications and the impossibility. Therefore, the related work present the impossibility to take great security measures in the communications between those devices. In our research, we demonstrate that using an IoT platform, which support the interconnection of heterogeneous and ubiquitous objects, and where communications are done via reader nodes. These objects can be like a smartphone, which takes information from a smartband or heart rate monitor, or an Arduino microcontroller that reads values from a thermostat or a rain sensor. These readers nodes are able to include the necessary measures that the communication through an insecure channel cannot be read by malicious users, preserving the users' privacy in the network.

2. State of the art

In the vision of the Internet of Things, there are innumerable objects connected to the Internet, transferring information from anywhere in the world and connecting to each other. This vision is as futuristic as troubling [1], because this way all of our