Connected Objects in Information Systems

Onyonkiton Théophile Aballo[1(✉)], Roland Déguénonvo[2(✉)], and Antoine Vianou[1,2(✉)]

[1] Doctoral School of Engineering Sciences, 01 BP 2009, Abomey-Calavi, Benin
onyonkiton.aballo@uac.epac.bj, avianou@yahoo.fr
[2] Abomey-Calavi University, LETIA-UAC, Cotonou, Benin
a_sessi@yahoo.fr

Abstract. The Internet of Things connects technical systems and sometimes also mechanical parts, electronic or even raw materials, with the web, via standardized communication interfaces. This opens up the ability to monitor and control devices and feeds for authorized users, as well as providing access to malicious people. Connected objects are also increasingly used for industrial applications. We are now talking about Industry with connected and intelligent factories to gain competitiveness. But these devices present intrinsic vulnerabilities and risks related to the new uses made possible thanks to an almost continuous connectivity to the Internet. There are actually very few areas of empirical testing currently. While waiting for a greater technological maturity of the Internet of Things, using supervision provides complete visibility of the entire network, which can greatly contribute to its security. The purpose of this article is to study objects connected to information systems.. . .

Keywords: Flow · Internet of Things · Risks · Vulnerabilities

1 Introduction

Nowadays, the internet has evolved to such an extent that it has become indispensable to life. At the very beginning, progress in the field of information and communication technologies plus, particularly the internet network and the services it offers, took place slowly but today innovation is occurring at a fast pace to the point of upsetting everyday life. In the same context, we can mention the appearance of connected objects, a new technology based on a combination of electronic equipment and smart software connected on the internet and offering services and applications ranging from the management of road traffic as a function of time and of the time in the field of transport, in the field of health. The development of communicating objects raises many issues related to the protection of information and communication systems that must guard against attacks and the diversion of their systems.

M. Serrhini et al. (Eds.): EMENA-ISTL 2019, LAIS 7, pp. 281–285, 2020.
https://doi.org/10.1007/978-3-030-36778-7_30

2 Connected Objects

A significant part of the billions of objects envisaged in the future will be measuring instruments, sensors, and remote actuators or communicating presence detectors. The table below compares the main technical characteristics of a connected object with those of office equipment (workstation and mobile, now well managed by the security of information systems). As shown in Table 1, above, the technical characteristics of connected objects are up to 1 million times lower than those of office equipment.

Table 1. Technical comparison of an internal connected object

	Object connected to networks	Operator	Workstation or mobile
RAM	100 ko	x20000	2 Go
Storage	256 ko	x1000000	256 Go
Frequency	32 MHz	x100	3 GHz
Consumption	10 Micronw	x1000000	10 W
Bandwidth	1 kbit/s	x10000	10 Mbit/s

3 Internet of Things

The Internet is a global network composed of several identifiable networks (public IP addresses) that can be reached through a standard communication protocol (TCP/IP), and an object is an element that cannot be precisely identified. Thus we can define the Internet of Things as a global element network communicating through a standard protocol. This approach shows two aspects of the Internet of Things (temporal and spatial) that allow people to connect from anywhere at any time through connected objects (Smartphone, tablets, sensors, CCTV cameras). The Internet of Things must be designed for easy use and secure manipulation to avoid potential threats and risks, while masking the underlying technological complexity.

Communication between objects is a model based on wireless communication between two objects. The information is transmitted through the integration of a wireless communication technology like ZigBee or Bluetooth (Fig. 1).

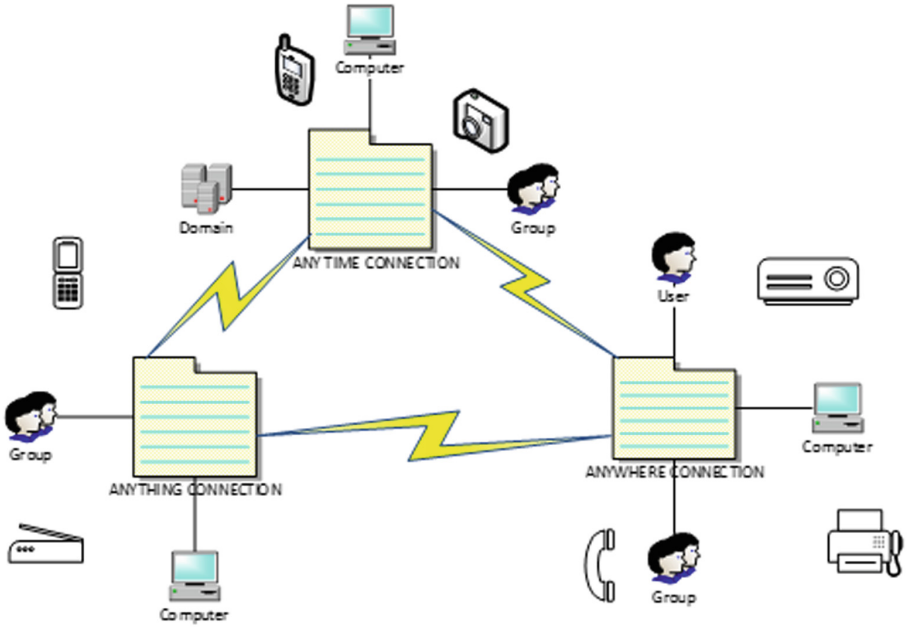

Fig. 1. Overview of a connected object environment

4 Areas of Implementation

Internet of Things applications touch virtually every area of life:

- Health and tele-monitoring systems;
- Connected agriculture to optimize the use of water;
- Connected vehicles to optimize urban traffic management;
- Appliances connected to optimize the consumption and distribution of electrical energy;
- Connected watches for well
- being and sport;
- Monitoring the temperature of a block within the laboratory
- Intrusion alert system in a server room- Automatic collection of symptoms in a patient
- Failure detection
- Smoke detection

To connect objects to information systems there are certain things to be aware of. It is:
-Traffic model where the probability of observing k arrivals during a time interval t is given by

$$Pk(t) = [(\beta t)t/k!]E - \beta t \quad (1)$$

where β is the arrival rate

- Access rate
- Debit generated by the signaling.

5 Risk in Terms of Security

Two major aspects are critical this is the security of data and drifts related to the use of these data. These risks can be translated in several ways:

- Theft of sensitive data for the benefit of a competitor or for blackmail,
- Loss of data on a hacked server, endangering some of the activities
- Loss of confidence following disclosure or loss of sensitive or private data,
- Involvement of industry materials in malicious acts with another of a third party.
- Like a computer or smartphone, a connected object has a network address that allows it to communicate. And even if its operating system is more minimalist, it has the same flaws as any other connected media. In other words, all connected objects can be the target of an attack.

6 Conclusion

The Internet of Things has enabled the development of a large number of applications endowing intelligence in a number of areas: health, home, city, television, automotive, industrial processes. The number of connected objects grows exponentially. Technical solutions have been developed to allow interoperability between different levels such as applications, cloud services, communication networks and smart sensor components to the computer system. Security issues are a critical point. In addition, the rise of the Internet of Things does not depend solely on the possibility of cooperating common objects equipped with microelectronics. It is essential that there are simultaneously reliable and secure infrastructures, economic and legal conditions of use and a social consensus on how new technical opportunities should be used.

References

1. Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., Yegin, A.: Protocol for Carrying Authentication for Network Access (PANA), RFC 5191, IETF, May 2008
2. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H.: Extensible Authentication Protocol (EAP), RFC 3748, IETF, June 2004
3. Pack, S., Choi, Y.: Pre-authenticated fast handoff in a public wireless LAN based on IEEE 802.1 x Model. Springer (2003)
4. Yeong, W., Howes, T., Kille, S.: Lightweight Directory Access Protocol, RFC 1777, IETF, March 1995

5. Sun, S., Reilly, S., Lannom, L., Petrone, J.: Handle System Protocol (ver 2.1) Specification, RFC 3652, November 2003
6. Hernández-Ramos, J.L., Jara, A.J., Marín, L.: DCapBAC: embedding authorization logic into smart things through ECC optimizations, Int. J. Comput. Math. (2016)
7. Shelby, Z., Hartke, K., Bormann, C.: The Constrained Application Protocol (CoAP), RFC 7252, IETF, June 2014
8. Internet of things research study 2015 report, Hewlett Packard (2015)