A contribution to security in IOT system. Reconfigurable Logic Device Technology and Fog Computing.

Osvaldo Marianetti[1], Pablo Godoy[1], Ernesto Chediak[1] and Carlos García Garino[1]

[1] Universidad Nacional de Cuyo. Facultad de Ingeniería, Mendoza, Argentina
olmarianetti@gamil.com, pablodgodoy@gmail.com,
ernestochediack@gmail.com, cgarcia@itu.uncu.edu.ar

Abstract. Internet of Things (IoT) presents a scenario in which billions of devices are interconnected and distributed almost anywhere, from the human being bodies to the most remote areas of the planet. In general, computer attacks, can steal or modify important data, bring down critical online services or obtain money illegally. On the other hand, in an IoT context, in addition to all these actions, there are possibilities of doing physical harm to people at a distance or manipulating critical infrastructures. This work proposes a FPGAs (Field Programmable Logic Array), with reconfiguration capabilities and great computational power, as a development alternative to the problems presented by the secure implementation of IoT systems.

Keywords: IoT, security, FPGA, reconfigurable.

1 IoT data security and integrity issues.

IoT augurs a very promising and interesting future. However, there are several security issues to be addressed: a) Technology heterogeneity: Protocol conversions are necessary to make compatible the security mechanisms implemented by different manufacturers; b) IoT computing capacity devices currently do not satisfy the by the security requirements available on other platforms; c) IoT communications are based mostly on wireless technologies.

This technology can suffer many different types of attacks, because the information exchange in IoT devices is quite predictable. Wireless sensor network (WSN) applications are a part of the IoT paradigm. WSN and the IoT share the same application scenarios. Sensor nodes within a WSN network can monitor and interact with each other just as physical and virtual objects do in IoT [1].

2 Wireless sensor network nodes. Design alternatives.

Wireless Sensor Networks (WSN) are based on groups of wireless connection embedded device nodes (sensors, microcontroller or processor plus a transmitter / receiver module, and so on). One of the main problems to be solved in practice is processing resources optimizing. WSNs uses nodes with general-purpose processors or microcontrollers in their deployment. General-purpose processors are designed to support virtually all types of applications. However, these tools are high priced and their power consumption is not optimized. In the literature the called *soft-core* processors (configurable architecture ones) have been proposed in order to circumvent the above cited drawbacks [2]. This choice optimizes the processor architecture so that it can be tailored to the needs of sensor network applications. There are FPGAs completely optimized on low-power. In the case of Xilinx and Altera, someone boards look promising since both are coupled with powerful specialized blocks and have a static power consumption between 41 mW and 197 mW. However, for applications with less advanced calculus at high-speed, the IGLOO platform [3] provides a limited static power consumption within the µW and the mW range. The costs of these devices have also dropped considerably.

3 FPGA technology at Fog Computing and Edge layer nodes.

Fog computing is a cloud technology than can be potentially useful in order to improve IoT deployment. The devices generated data are not uploaded directly to the cloud. Instead, the information is preprocessed first in smaller decentralized data centers. This concept encompasses a network that extends from its own limits, where the terminals or sensors generate the data, to the central destination of the data in the public or private cloud or in a proper data center.

The goal of fog computing is to shorten the communication paths between the cloud and the devices in order to reduce the throughput of data on external networks. The nodes fulfill the role of intermediate layer in the network in which it is decided which data are processed locally or remotely. The three layers of a Fog computing infrastructure are:

a) Edge layer: comprises all the smart devices, place at the edge of the network, of an IoT architecture. The data that generated in this layer is processed in the same node or is to send to a server in the fog layer.

b) Fog layer: it is based on a proper quantity of high-performance servers that receive the data from the first layer, prepare and send it to the cloud if necessary.

b) Cloud layer: the cloud layer is the upper layer of a fog computing architecture.

In fog computing the resources for data storage and preparation are distributed in the intermediate layer in the network by means of fog nodes or pre-processing units. Security issues are usually approached considering traditional solutions. A wider security vision is required from the design, where threats are addressed proactively. Reconfigurable logic technology can enable efficient, scalable, and sustainable solutions in this case. The great computational capacity of FPGAs together the possibility to process different types of information, offer a response to address the following requirements:

a) Capacity and dynamic load management: FPGAs allow the resources available for a given task to be adapted at runtime without complex infrastructures.

b) Security: Due to the nature of reconfigurable hardware, the system is more resistant to attacks. In addition, more powerful encryption hardware systems based can be added without affecting the operation of the application [4].
c) Software infrastructure simplification: All the functionality of the Fog IoT node can be included on a FPGA. Then the maintainability and operating cost of the platform are improved.

4 FPGA based WSN and edge layer nodes prototypes.

The design of an architecture of an embedded system based on soft_processors is discussed in this section. The approach for an architecture of a WSN and/or Edge node based on traditional components can be seen in Figure 1. The main drawback of this approach is that components are not reconfigurable and cannot be adapted for flexible working conditions.

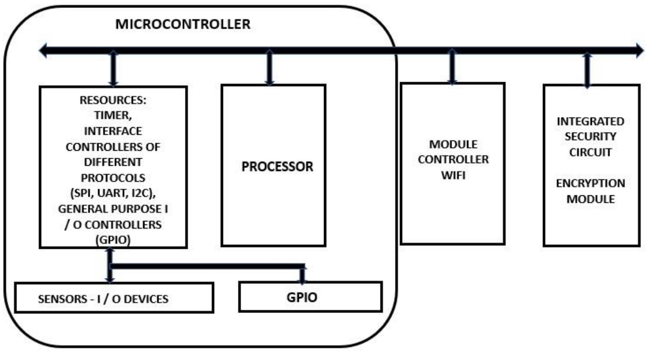
MICROCONTROLLER
RESOURCES: TIMER, INTERFACE CONTROLLERS OF DIFFERENT PROTOCOLS (SPI, UART, I2C), GENERAL PURPOSE I / O CONTROLLERS (GPIO)
PROCESSOR
MODULE CONTROLLER WIFI
INTEGRATED SECURITY CIRCUIT
ENCRYPTION MODULE
SENSORS - I / O DEVICES
GPIO

Figure 1. Architecture of a WSN and/or Edge node based on traditional components.

FPGAs is a valuable alternative in order to improve the operability of WSN nodes as has been previously considered in sections 2 and 3. On the other hand, the implementation of FPGA based nodes on the Edge layer can improve the security of the overall system. The proposed architecture has the same functionality of commercial systems including security components in its design, while the characteristics of the nature of reconfigurable hardware are implicitly considered. Then the system is more resistant to attacks. In FPGA-based architecture, its functional units (memories, ports, controllers, timers, etc.) are reconfigurable and adaptable to new requirements, even remotely. A FPGA based architecture [5] scheme is presented in Figure 2. For the development of the embedded system the Quartus II development environment (versions 13.1 web edition and Quartus Prime Lite Edition 17.0) has been used. The QSYS tool of these environments for the generation of the SOPC (system programmable on chip) and the NIOS II software build tool for Eclipse environment have been used for programming the NIOS II / e soft_processor. In a previous work [6] the authors have designed a FPGA based WSN processor node.

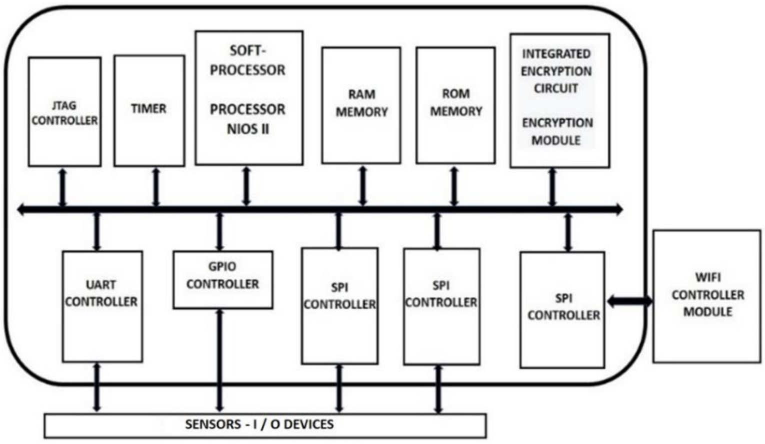

Figure 2. System embedded in reconfigurable hardware.

5. Conclusion.

The proposed prototype can be considered as a proof of concept that allows to research architectures of programmable systems on chip (SOPC) based on FPGAs. This protoype can be optimized in order to operate as a node of a WSN and also in applications of IoT systems. For instance, the proposed tool can be used in order to implement gateways or nodes of the Edge layer [7].

References

1. Baktyan, A. A., & Zahary, A. T. A Review on Cloud and Fog Computing Integration for IoT: Platforms Perspective. EAI Endorsed Transactions on Internet of Things. (2018).
2. Lei Zhou, Qingxiang Liu, Bangji Wang, Peixin Yang, Xiangqiang Li and Jianqiong Zhang. Remote System Update for System on Programmable Chip Based on Controller Area Network. School of Physical Science and Technology, Southwest Jiaotong Universit. (2017).
3. IGLOO platform. https://www.mdpi.com/1424-8220/12/9/12235/pdf
4. A Lattice Semiconductor White Paper IoT Sensor Connectivity and Processing with Ultra-Low Power, Small Form-Factor FPGAs. (2018).
5. O. Marianetti, P. Godoy, E. Chediak, D. Fontana. La tecnología de lógica reconfigurable como alternativa en la solución a los problemas de seguridad en IoT. XXVI Jornadas de investigación: "Avances y desafíos de la ciencia en pandemia". UNCUYO. (2020).
6. O. Marianetti, A. Iglesias, L. Arce. Diseño de un prototipo de procesador soft-core para aplicaciones en nodos de WSN. https://doi.org/10.18682/cyt.v1i17. Online ISSN 2344-9217 | Print ISSN 1850-0870. Universidad de Palermo. Facultad de Ingeniería (2017)
7. Jhansi Naga Sai Surekha, Archana, Hannah Priyanka, Munavvar Hussain. Raju Institute of Technology, Narsapur, India. "An FPGA Implementation of Health Monitoring System using IOT.".http://ijcrt.org/papers/IJCRT_185534.pdf