TECNOLOGÍA DE DISPOSITIVOS DE LÓGICA RECONFIGURABLE APLICADA EN LA IMPLEMENTACIÓN SEGURA DE SISTEMAS DE IOT

Osvaldo L. Marianetti [(1)(2)], Pablo D. Godoy [(1)], Ernesto E. Chediak[(1)], Daniel S. Fontana[(1)], Carlos García Garino[(1)]

[(1)] Universidad Nacional de Cuyo. Facultad de Ingeniería. [(2)] Universidad de Mendoza. Facultad de Ingeniería.

olmarianetti@gmail.com, pablodgodoy@gmail.com, ernestochediack@gmail.com, danielsantiagofontana@gmail.com, cgarcia@itu.uncu.edu.ar

RESUMEN

Internet de las Cosas (IoT) presenta un escenario en el cual miles de millones de dispositivos se encuentran interconectados y distribuidos por casi cualquier lugar, desde el cuerpo de un ser humano hasta las áreas más remotas del planeta. Gracias al abaratamiento de los costos de los microprocesadores, al aumento de las capacidades de cómputo y a las nuevas tecnologías inalámbricas, se prevé en 2021 más de 50.000 millones de dispositivos conectados. Los ataques informáticos en general, pueden robar o modificar datos importantes, hacer caer servicios críticos online o conseguir dinero de forma ilícita. En cambio, en un contexto de IoT, además de todas estas acciones, existen posibilidades de hacer daño físico a personas a distancia y/o manipular infraestructuras críticas.

Este proyecto propone demostrar que, a partir del paradigma de Computación en la Niebla, los dispositivos lógicos programables como las FPGA (Field Programmable Logic Array), con capacidades de reconfiguración y gran potencia computacional, más la posibilidad de adaptar el procesamiento al tipo de información que presente en estas aplicaciones (eventos, imágenes, etc.), se pueden considerar una alternativa de desarrollo frente a las problemáticas que presenta la implementación segura de sistemas de IoT.

Palabras clave: IOT, seguridad, FPGA, reconfigurable.

CONTEXTO

Desde la Secretaría de Investigación, Internacionales y Posgrado se desarrollan convocatorias a proyectos bienales que tienen por finalidad la promoción de la investigación científica y tecnológica.

Este proyecto está inserto en la convocatoria Proyectos de investigación SIIP 2019, http://www.uncuyo.edu.ar/ciencia_tecnica_y_posgrado/proyectossiip2019.

1. INTRODUCCIÓN

Internet de las Cosas (IoT) o la evolución a IOE (M2M, P2M Y M2P) presenta un escenario en el cual miles de millones de dispositivos se encuentran interconectados y distribuidos por casi cualquier lugar. Podemos imaginar un mundo donde todos los objetos tienen identidad propia, desde una cafetera, un auto que se prepara para arrancar o un servicio médico capaz de monitorizar la salud de un individuo salud en forma remota. Internet de las cosas facilitará el despliegue de ciudades inteligentes, Industria 4.0, vigilancia inteligente y grandes cambios en la gestión de infraestructuras, agricultura, medicina y casi cualquier otro sector económico.

En el marco de lo que se denomina la nueva Revolución Industrial o Industria 4.0, se hace referencia al concepto de “smart factory”. En

el concepto de la fábrica inteligente, una planta industrial completamente conectada, la cual podría generar diariamente varios centenares de gigabytes, volúmenes enormes de información que dificultarían su procesamiento en la nube o en de forma centralizada. Estos requerimientos permiten replantear la infraestructura actual de la nube tal como la conocemos.

Una alternativa que propone posibles soluciones a la problemática que acompaña la implantación total de la IoT, se conoce como computación en la niebla (fog computing). [1]

Fog computing es el nombre de una tecnología cloud por la cual los datos que generan los dispositivos no se cargan directamente en la nube, sino que se preparan primero en centros de datos descentralizados más pequeños. El concepto engloba a una red que se extiende desde sus propios límites, que es donde los terminales o sensores generan los datos, hasta el destino central de los datos en la nube pública o en un centro de datos o nube privada.

El objetivo de la computación en la niebla es acortar las vías de comunicación entre la nube y los dispositivos y reducir el caudal de datos en redes externas. Los nodos cumplen el rol de capa intermedia en la red en la que se decide qué datos se procesan localmente y cuáles se envían a la nube o a un centro de datos para ser analizados o procesados. Las tres capas (layer) de una infraestructura de computación en la niebla son:

- Edge layer: la capa del borde comprende a todos los dispositivos inteligentes (dispositivos en el borde de la red) de una arquitectura de IoT. Los datos que se generan en esta capa se procesan en el mismo terminal o se envían a un servidor (nodo fog) en la capa niebla.
- Fog layer: la capa en la niebla está compuesta por una serie de servidores de gran rendimiento que reciben los datos de la primera capa, los preparan y los envían a la nube si es necesario.
- Cloud layer: la capa en la nube constituye el punto final de una arquitectura de fog computing.

En la fog computing los recursos para el almacenamiento y la preparación de los datos abandonan la nube pública o el centro de datos y se distribuyen en una capa intermedia en la red por medio de nodos fog o unidades de preprocesamiento.[2]

El OpenFog Consortium, que reúne a algunas de las empresas e instituciones académicas más innovadoras del sector con el objetivo de desarrollar un marco común de desarrollo de la tecnología, está trabajando en una arquitectura de referencia para sistemas de fog computing.

La computación en la niebla se diferencia de la tecnología cloud, sobre todo, por el lugar donde se accede a los recursos y se procesan los datos. La computación en la nube suele basarse en centros de datos centralizados. Aquí, los servidores en el backend son los que suministran recursos como la potencia de procesamiento y la memoria, que utilizan los clientes a través de la red. La comunicación tiene lugar entre dos o más terminales siempre mediante un servidor en un segundo plano.

Con conceptos como el de la fábrica inteligente esta arquitectura tiene limitaciones, puesto que en ella hay un gran número de dispositivos que están intercambiando datos constantemente. Apoyándose en el procesamiento de los datos cerca de la fuente, la computación en la niebla logra reducir el tráfico de datos.

Pero la computación en la nube no solo se ve saturada por el tráfico de datos que generan las grandes infraestructuras de IoT, sino también por la latencia, porque el procesamiento centralizado de los datos implica depender de las rutas de transferencia y esto ocasiona siempre cierto desfasaje. Los dispositivos y los sensores han de estar siempre en contacto con el servidor en el centro de datos para poder comunicarse y esperar tanto el tratamiento externo de la petición como la propia respuesta, de modo que este tiempo de latencia se convierte en un problema en procesos de fabricación apoyados en IoT que necesitan el procesamiento inmediato de la información

para que las máquinas puedan reaccionar inmediatamente a cualquier incidente.
La fábrica inteligente no es el único campo de aplicación en que la computación en la niebla puede aportar sus ventajas. Otros proyectos como los autos semiautónomos o completamente autónomos, o la ciudad inteligente, integrada por redes inteligentes de suministro, también necesitan que los datos se analicen en el momento. Un coche inteligente, por ejemplo, está constantemente recogiendo datos sobre el entorno, las condiciones de conducción y la situación del tráfico que se han de evaluar sin latencia para que pueda reaccionar ante cualquier imprevisto de la forma correcta. La computación en la niebla permite procesar los datos del vehículo tanto en el automóvil mismo como en el proveedor del servicio.
IoT augura un futuro muy prometedor e interesante, pero respecto a lo relacionado a la seguridad, la evolución no presenta el mismo nivel de progreso. [3]
Existen varias organizaciones y gobiernos que están promoviendo y obligando a que la seguridad esté presente desde el diseño de los dispositivos, forzando a los fabricantes a que tengan en cuenta todos los aspectos. (Congreso de los EEUU, Department of Homeland Security y National Science Foundation)
Los principales problemas de seguridad del Internet de las Cosas son:
1. La heterogeneidad de tecnologías. Son necesarios conversiones de protocolos y hacer compatibles los mecanismos de seguridad implementados por distintos fabricantes.
2. Los dispositivos IoT no cuentan en la actualidad con la capacidad de computación que requieren las medidas de seguridad que se adoptan en otras plataformas.
3. Las comunicaciones de toda la tecnología IoT se soporta casi totalmente en el aire, es decir comunicaciones inalámbricas. Esta es la tecnología que más tipos de ataque puede sufrir, cuando precisamente el intercambio de información de los dispositivos IoT son bastante predecibles y su arquitectura y formato no son fáciles de cambiar.

Las soluciones tradicionales donde la seguridad se aplica como una ocurrencia posterior y como un parche contra los ataques conocidos son insuficientes. Se requiere una visión de seguridad desde el diseño, donde las amenazas se abordan de forma proactiva. [4]
La tecnología de lógica reconfigurable es un prestador de soluciones eficientes, escalables y sostenibles. La gran capacidad computacional de las FPGA y la posibilidad de adaptar el procesamiento a distintos tipos de información, y las propiedades que se citan a continuación, también ofrecen una respuesta a las necesidades planteadas:
Gestión de la capacidad y carga dinámica: las FPGAs permiten adaptar en tiempo de ejecución los recursos disponibles para una determinada tarea sin complejas infraestructuras
Seguridad: debido a la naturaleza del hardware reconfigurable, el sistema es más resistente a ataques. Además, pueden añadirse sistemas de encriptación más potentes que se ejecuten en hardware sin afectar al funcionamiento de la aplicación. [5]
Simplificación de la infraestructura software: mejora la mantenibilidad y el costo operativo de la plataforma. Toda la funcionalidad del nodo fog (concentrador o puerta de enlace) IoT puede implementarse en una FPGA.

2. LINEAS DE INVESTIGACIÓN y DESARROLLO

Los ejes del tema de investigación del proyecto son:
a) Identificar los principales problemas de seguridad en los dispositivos utilizados en plataformas de IoT.
b) Investigar las características de los dispositivos lógicos programables FPGA que cumplen con los requerimientos de capacidad de cómputo.
c) Demostrar experimentalmente la vulnerabilidad de dispositivos IOT. (En particular en redes de sensores inalámbricos)
d) Desarrollar arquitecturas de sistemas programables en un chip (SOPC) con

dispositivos reconfigurables, FPGAs, optimizadas para operar como nodo de una red de sensores inalámbricos y/o como nodo de la capa de borde en aplicaciones de sistemas de IoT y que pueda interactuar con concentradores o nodos de la capa fog, utilizando tecnologías y herramientas de disponibles y accesibles en el contexto local.

3. RESULTADOS OBTENIDOS/ESPERADOS

Los resultados obtenidos son:

1-Diseño de un prototipo de procesador soft-core para aplicaciones en nodos de WSN. [6]

Unos de los problemas a resolver en las WSN es la optimización del consumo de energía disponible en los nodos, de modo de lograr el máximo tiempo de vida útil de la red, optimizar los recursos de procesamiento y adecuar los nodos a la topología dinámica de la red.

Las WSN utilizan en su despliegue nodos con procesadores o microcontroladores de propósito general. Como alternativa a estos, se implementó un prototipo de procesador soft-core. Esto optimiza la arquitectura del procesador para que se pueda adaptar a las necesidades de las aplicaciones de las redes de sensores. Por lo tanto, el procesador puede contar con sólo aquellos componentes de hardware requeridos por la aplicación particular y así reducir el consumo de energía del procesador. Además, el procesador soft-core puede ser integrado en un chip con los otros componentes de hardware necesarios para desarrollar el nodo sensor.

Se desarrolló la descripción mediante código VHDL del prototipo de procesador soft-core. Se concretó la síntesis de este diseño y se programó en un dispositivo FPGA. El funcionamiento de la implementación se verificó con entidades de test con estímulos. Estos correspondían a carga de registros y accesos a memoria, como así también operaciones aritméticas.

El prototipo ofrece en principio una mayor velocidad de procesamiento que un microcontrolador de propósito general con una implementación más simple (se comparó con 4 microcontroladores comerciales).

Deben considerarse mejoras en la arquitectura, como instrucciones de manejo de bits e incorporar módulos de interface para comunicación con sensores.

2- Vulnerabilidad de los dispositivos utilizados en aplicaciones de IoT. [7]

Se desarrolló un equipo de control de condiciones ambientales. Este sistema se implementó utilizando dispositivos de uso frecuente en hogares y oficinas, que cuentan con sensores, los que podrían ser vulnerables a un uso inadecuado. El producto final tiene por objetivo la medición de los siguientes parámetros ambientales: temperatura, humedad, iluminación, nivel de ruido, y presencia.

El funcionamiento del equipo responde a la consigna de medir los parámetros ambientales y transmitirlos mediante WIFI a una plataforma en la Nube utilizando un protocolo UDP. El firmware embebido en el dispositivo, tiene una rutina principal que realiza una lectura de los sensores conectados por una interface I2C, realizando una actualización de los valores cada 30 segundos. Por otra parte, en el desarrollo del sistema se programó una subrutina embebida en el código que realiza la lectura un puerto analógico, conectado a la salida analógica del micrófono disponible en la placa de sensores. A los usuarios del sistema solo se les da acceso a la parte de la plataforma que presenta los parámetros ambientales. Quienes desarrollaron el equipo pueden tener acceso pleno al sonido de la habitación en donde se encuentra instalado el sensor.

El experimento desarrollado demuestra la vulnerabilidad de los elementos que en la actualidad se utilizan en las aplicaciones de IoT, sino se considera la problemática de la seguridad desde el diseño del sistema.

3-Sistema embebido basado en soft_processors. [8]

Se ha diseñado una arquitectura de un sistema embebido basada en soft_processors. Esta arquitectura presenta la misma funcionalidad de los sistemas comerciales con componentes

de seguridad en su diseño, pero puede incorpora las características de la naturaleza del hardware reconfigurable, para que el sistema sea más resistente a ataques. En la arquitectura basada en FPGA sus unidades funcionales (memorias, puertos, controladores, temporizadores, etc.) son reconfigurables y adaptables a nuevos requerimientos, incluso en forma remota.[9] [10]

Para el desarrollo de la arquitectura del sistema embebido basada en soft_processors, se ha utilizado el entorno de desarrollo Quartus II (versiones 13.1 web edition y Quartus Prime Lite Edition 17.0) La herramienta QSYS de estos entornos para le generación del SOPC (sistema programable en el chip) y el entorno NIOS II software build tool for Eclipse para la programación del soft_processor NIOS II/e.

En esta implementación se debe concluir con el desarrollo del módulo de encriptación del SOPC.

Resultados esperados:

Verificar el funcionamiento del SOPC desarrollado como nodo WSN y como nodo de la capa de borde.

Desarrollar una arquitectura de nodo Fog basada en diseño SOPC sobre tecnología FPGA.

4. FORMACIÓN DE RECURSOS HUMANOS

La estructura del equipo de trabajo actual es: Dos doctores: Dr. García Garino y Dr. Godoy. Un magister: Mgt Marianetti (actual doctorando) y dos ingenieros: Ing. Chediak e Ing. Fontana.

Los conocimientos y experiencias resultantes, debidamente mediados, podrán ser transferidos directamente a los alumnos de la carrera Licenciatura en Ciencias de la Computación, que se dicta en la Facultad de Ingeniería de la Universidad Nacional de Cuyo, ya que todos los integrantes de este proyecto son profesores de diferentes materias de dicha carrera (Arquitectura de Computadoras, Arquitecturas Distribuidas, Redes), y los temas sobre los que se va a nvestigar, articulan con los programas de estudios de varias asignaturas de dicha carrera, cuyo cursado comenzó en el año 2017.

En el presente hay una tesis posgrado en curso.

5. BIBLIOGRAFÍA

[1] Baktyan, A. A., & Zahary, A. T. (2018). A Review on Cloud and Fog Computing Integration for IoT: Platforms Perspective. EAI Endorsed Transactions on Internet of Things.

[2] Tatiana Delgado Fernández. Un acercamiento a fog computing (Computación en la niebla). https://sistemas.acis.org.co/index.php/sistemas/article/download/121/94.

[3] IoT Security White Paper 2018 – Huawei. https://www.huawei.com/.../iot/.../iot_security_white_paper_2018

[4] Restuccia, F., D'Oro, S., & Melodia, T. (2018). Securing the Internet of Things: New Perspectives and Research Challenges. https://arxiv.org/abs/1803.05022.

[5] A Lattice Semiconductor White Paper IoT Sensor Connectivity and Processing with Ultra-Low Power, Small Form-Factor FPGAs. 2018.

[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

[7] O. Marianetti, Pablo D. Godoy, E. Chediak, Daniel S. Fontana. Vulnerabilidad de los dispositivos utilizados en aplicaciones de IoT. CASE 2019. Libro de Trabajos. P. 135. ISBN 978-987-46297-6-0)

[8] O. Marianetti, Pablo D. Godoy, E. Chediak, Daniel S. Fontana. La tecnología de lógica reconfigurable como alternativa en la solución a los problemas de seguridad en Internet de las Cosas. XXVI Jornadas de investigación: "Avances y desafíos de la ciencia en pandemia". 2020. UNCUYO.

[9] Saar Drimer, Markus G. Kuhn. A Protocol for Secure Remote Updates of FPGA

Configurations.. Computer Laboratory, University of Cambridge. 2018.
[10] 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 University, 2017.