DISEÑO Y CONSTRUCCIÓN DE SISTEMAS DE IOT SEGUROS Y ESCALABLES

Sebastián U. Flores, Mario Berón , Daniel Riesco, Pedro Rangel Henriques
Departamento de Informática - Facultad de Ciencias Físico Matemáticas y Naturales - Universidad Nacional de San Luis - Ejército de Los Andes 950 - San Luis – Argentina
Universidade do Minho Braga - Portugal
sebastian.ur.flores@gmail.com, {mberon,driesco}@unsl.edu.ar
pedrorangelhenriques@gmail.com

RESUMEN

En la actualidad, tanto los avances en las tecnologías de la información y de la comunicación como la reducción de costos y tamaño de los dispositivos electrónicos, han impulsado el surgimiento de nuevos servicios que conectan el entorno, con redes informáticas. Estos progresos han posibilitado la extracción de información y la realización de cambios en el entorno, a través de diversos tipos de sensores y actuadores. Esta clase de servicios conforman una nueva rama de las tecnologías conocida como IoT, que abarca una amplia cantidad de áreas de investigación y que busca fundamentalmente una mejora en la calidad de vida de las personas, un incremento de la eficiencia de los procesos industriales y un mayor cuidado del medio ambiente y de sus recursos, transformando para ello la forma en que interactúan las personas con el entorno.

En este artículo, se presenta una línea de investigación que aborda el diseño y construcción de *sistemas de IoT Escalables y Seguros*. Un sistema de IoT está conformado por personas y por dispositivos compuestos por sensores y actuadores, en el cual las partes componentes interactúan entre sí, manteniendo un cierto grado de interdependencia para el correcto funcionamiento del sistema. La heterogeneidad antes mencionada hace que la escalabilidad y seguridad de los sistemas de IoT presenten importantes desafíos de investigación.

PALABRAS CLAVE

Sistema de IoT, Dispositivo IoT, Escalabilidad, Seguridad, Privacidad, Arquitectura, Machine to Machine.

CONTEXTO

La presente línea de investigación se enmarca en dos Proyectos de Investigación. El primero: “Ingeniería de Software: Conceptos, Prácticas y Herramientas para el desarrollo de Software con Calidad” – Facultad de Ciencias Físico-Matemáticas y Naturales, Universidad Nacional de San Luis. Proyecto N.º P-031516. Tal proyecto es la continuación de diferentes proyectos de investigación, a través de los cuales se ha logrado un importante vínculo con distintas universidades a nivel nacional e internacional. Además, se encuentra reconocido por el Programa de Incentivos. El segundo proyecto: “Fortalecimiento de la Seguridad de los Sistemas de Software mediante el uso de Métodos, Técnicas y Herramientas de Ingeniería Reversa” realizado en conjunto con la Universidade do Minho Braga, Portugal, fue recientemente aprobado por el Ministerio de Ciencia, Tecnología e Innovación Productiva (MinCyT), y su código es PO/16/93.

1. INTRODUCCIÓN

El término IoT es la abreviación de la frase en inglés “Internet of Things” (Internet de las Cosas). Este término corresponde a un dominio de aplicación que integra diferentes campos tecnológicos y sociales. De acuerdo con la IEEE [1], a pesar de que en los últimos años se han realizado grandes avances en este dominio de aplicación, aún no se ha alcanzado un consenso en cuanto a una definición del mismo, que contenga todas sus características y pueda facilitar una mejor comprensión de esta tecnología emergente.

De acuerdo a lo expuesto por la IEEE en [1], el software es un factor muy importante para los sistemas de IoT:

- Los sistemas operativos de IoT están diseñados para ejecutarse en componentes de pequeña escala de la manera más eficiente posible, mientras que, al mismo tiempo, proporcionan funcionalidades básicas para simplificar y respaldar los objetivos y propósitos de las aplicaciones [6,8,15].
- Al contar con una capacidad de procesamiento reducida y con escaso almacenamiento, es muy importante el desarrollo de interfaces de programación de aplicaciones (APIs) que fomenten la reutilización de componentes y una adecuada gestión de los datos que minimice los costos de almacenamiento y de procesamiento [6,7,9,10].
- Los sistemas de IoT, potencialmente pueden crecer y llegar a componerse por millones de dispositivos diferentes, cada uno ubicado en regiones remotas del planeta y con usuarios ubicados también remotamente. En este contexto, la autogestión y auto-optimización de cada dispositivo y / o subsistema individual pueden ser requisitos importantes. En otras palabras, los comportamientos autonómicos podrían convertirse en la norma en sistemas de IoT grandes y complejos [2,6,8,10,13].
- Debido a que los sistemas de IoT producen y manejan información reservada, garantizar la seguridad y privacidad de los datos debe ser considerado prioritario desde los comienzos de su planificación e implementación, de forma que ambas estén integradas en cada proceso del sistema [4,10,11,12,13,14].
- Para garantizar la escalabilidad de un sistema de IoT, este debe poseer un diseño arquitectónico adecuado. Por la característica previamente mencionada, se entiende la creación de un sistema flexible que permita interconectar tantos dispositivos IoT como sea necesario. Dicha conexión se realiza sin que importe el medio de conexión físico o el sistema operativo que posea cada uno de ellos, siempre y cuando utilicen las interfaces de software y protocolos de comunicación adecuados [2,5,6,13].
- Finalmente, los sistemas de IoT pueden tener diferentes niveles de impacto en las personas y la sociedad en la que viven, por lo que deben ser concebidos y conducidos dentro de las restricciones y regulaciones de cada país.

Algunos ámbitos de aplicación de sistemas de IoT son los siguientes:

- Sistemas de domótica.
- Extracción y análisis automáticos o semi automáticos de datos en líneas de producción industrial, que permitan optimizar los procesos de negocio [3].
- Dispositivos capaces de ser vestidos por personas o animales, que permitan monitorear el estado físico de los mismos o que les permitan extender sus capacidades físicas (el término más común asociado a esta clase de dispositivos, a nivel mundial, es el de wearables).
- Dispositivos de monitoreo de cultivos y riego automático e inteligente.

Los sistemas de IoT no necesariamente requieren de interacción humana en su funcionamiento. ETSI [2] trata esta clase de interacciones al definir las comunicaciones *"Machine-to-Machine (M2M)"* (en español, comunicaciones Máquina a Máquina). Las comunicaciones M2M son aquellas realizadas directamente entre dispositivos y / o subsistemas de IoT, con interacción humana escasa o nula. Esta clase de comunicación posee varias aplicaciones:

- Automatización de decisiones de carácter determinístico, las cuales se encuentran totalmente estudiadas y no requieren de intervención humana.
- Aprendizaje de patrones de comportamiento humano o patrones en el funcionamiento de procesos propios del sistema. En este caso, la única interacción humana que podría presentarse es la del encargado de supervisar los resultados del aprendizaje realizado por el sistema.
- Autonomización de un sistema aislado, localizado en una ubicación de difícil acceso para seres humanos.
- Edificios inteligentes que se adapten automáticamente a las condiciones del entorno.

En este caso, existiría una constante comunicación entre subsistemas de IoT distribuidos en todo el edificio y sus alrededores, cada uno evaluando las condiciones de su propio entorno y comunicando los cambios relevantes al resto de los subsistemas, para que cada uno se adapte de la mejor forma a las mismas.

Por todo lo mencionado en los párrafos anteriores, se puede notar que es difícil la creación de un marco general de trabajo que permita desarrollar e integrar sistemas de IoT de diversa escala y con ámbitos de aplicación heterogéneos. Este marco debe ser lo suficientemente flexible como para permitir todo tipo de modificación estructural del sistema, de una forma comprensible y segura. También, debe permitir la obtención de múltiples vistas que permitan analizar diferentes propiedades del sistema. Para crear este marco de trabajo, es necesario detectar y comprender los problemas a los que se enfrentan los arquitectos y desarrolladores de sistemas de IoT y que, de acuerdo con Kranz et al. [3], llevan a que un 60% de las iniciativas IoT se estanquen en la fase de prueba de concepto, y del 40% restante, sólo el 26% sean consideradas un completo éxito.

Algunos de los problemas antes mencionados son los siguientes:

- Crecimiento organizado del sistema, pudiendo este gestionar a tantos dispositivos y usuarios como sea necesario, sin importar la ubicación geográfica de los mismos y, minimizando los costos de desarrollo y los riesgos asociados al crecimiento del sistema [5,7].
- Establecimiento de jerarquías entre dispositivos, con el fin de que las comunicaciones se realicen de forma controlada y facilitando el posterior procesamiento de la información comunicada.
- Establecimiento de jerarquías de usuarios, asignando a cada uno un determinado nivel de acceso a los dispositivos del sistema de IoT y a la administración del mismo.
- Soporte por software que simplifique la conexión entre dispositivos con múltiples interfaces de hardware y protocolos diferentes [2].
- Soporte para visualizar el flujo de la información en el sistema de IoT, de una forma global, o local de cada subsistema que lo conforme.

Para concluir esta introducción, es importante mencionar que se prevé un amplio crecimiento en la cantidad de objetos conectados a internet a través de sistemas de IoT. Kranz et al. estima que, en el año 2020, se alcanzará una cifra de 50.000 millones de objetos conectados en todo el mundo [3].

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

En la actualidad, existe una gran variedad de sistemas operativos destinados a dispositivos IoT (e.g. TinyOS, Linux, RIOT, CONTIKI, Windows 10 IoT Core) [1,15]. También, existe una gran cantidad de librerías y aplicaciones implementadas con el fin de brindar soporte a desarrolladores de sistemas de IoT.

De acuerdo con IEEE [1], frente al crecimiento en la cantidad de *cosas conectadas a internet* (i.e. dispositivos IoT), cada una perteneciendo posiblemente a diferentes *dominios de administración* (i.e. diferentes sistemas/subsistemas de IoT), es necesario repensar por completo los enfoques tradicionales en el desarrollo de aplicaciones web, siendo prioritarios elementos como la escalabilidad y la lógica distribuida.

Coincidiendo con IEEE [1], mientras que IoT promete una mejor vida a través de dispositivos conectados y de la información y métricas que ellos generen, también marca el comienzo de una nueva era en cuanto a la privacidad y la seguridad. Según OWASP [4], uno de los nuevos riesgos de seguridad asociados con IoT, son los llamados *ataques de superficie*, que explotan las fallas de seguridad de los sistemas de IoT para vulnerar a empresas, gobiernos, organizaciones y a usuarios particulares.

Frente a lo mencionado en los párrafos anteriores, está claro que los desarrolladores de sistemas de IoT se enfrentan a un problema principal: *la creación de un sistema de IoT escalable y seguro*.

Esta línea de investigación propone:

- Hacer una investigación profunda sobre las vulnerabilidades de seguridad que afectan a los sistemas de IoT.
- Investigar el estado del arte de los patrones/estilos arquitectónicos de sistemas de IoT, y de los protocolos utilizados en su desarrollo.
- Integrar las investigaciones realizadas con el fin de crear un conjunto de herramientas que faciliten al desarrollador la creación de sistemas de IoT escalables y seguros, brindando soporte en la integración de subsistemas que posiblemente estén ubicados en diferentes posiciones geográficas, posean diferentes sistemas operativos y utilicen diferentes protocolos de software y hardware.

3. RESULTADOS OBTENIDOS/ESPERADOS

Con el objetivo de evaluar los conceptos investigados, se realizó un sistema de prueba, compuesto por los siguientes componentes:

- Una aplicación para Windows, destinada a los usuarios del sistema de IoT. Esta aplicación provee un sistema automatizado de búsqueda que muestra en pantalla todos los dispositivos IoT conectados en la red Wi-Fi local. A continuación, ofrece al usuario la posibilidad de diseñar la arquitectura del sistema de IoT, utilizando todos los dispositivos que fueron encontrados en la búsqueda. Durante esta etapa, el usuario puede:
    - Establecer comunicaciones M2M [2] entre los distintos dispositivos IoT detectados.
    - Definir cuales datos deben ser transmitidos periódicamente desde los dispositivos hacia la aplicación del usuario.
    - Determinar cuáles datos deben ser almacenados por los dispositivos para la obtención de métricas.

  Una vez finalizado el diseño arquitectónico, la aplicación automáticamente establece conexión con los dispositivos y les transmite la configuración establecida por el usuario desde la aplicación.
- Una placa Arduino conectada a varios sensores, junto con un transmisor/receptor Wi-Fi, para que esta pudiera conectarse a la red Wi-Fi local. A continuación, se la programó para que sea compatible con los protocolos utilizados dentro del sistema de IoT y se la conectó a la red Wi-Fi local. Por último, se ejecutó la búsqueda automática en la aplicación del usuario y se comprobó que la placa Arduino se conectó exitosamente al sistema de IoT.
- Dado que se contaba con una única placa Arduino y se deseaba probar la configuración del sistema con más de un dispositivo IoT, se creó un script en Python que simula la ejecución de tales dispositivos. Cada vez que se ejecuta el script, se obtiene un nuevo dispositivo IoT conectado a la red Wi-Fi local, preparado para interactuar utilizando los protocolos del sistema. Se ejecutó nuevamente la búsqueda automática en la aplicación del usuario, pudiendo comprobar que todos los dispositivos simulados se conectaban exitosamente al sistema.
- Se definieron protocolos para la conexión y desconexión entre componentes del sistema de IoT (e.g. dispositivos IoT, aplicaciones de usuario), el establecimiento de configuraciones desde la aplicación de usuario hacia los dispositivos IoT, y la transmisión de mensajes básicos (e.g. el valor medido por un sensor, la asignación de una orden a un actuador).

A futuro se poseen los siguientes objetivos:

- Realizar una investigación profunda acerca de las amenazas de seguridad que afectan a los sistemas de IoT.
- Extender el conjunto de protocolos para cubrir todos los procesos posibles de un sistema de IoT, de una forma que garantice la seguridad del sistema y la privacidad de sus datos.
- Crear patrones de diseño arquitectónico que puedan ser usados en diferentes ámbitos de aplicación de sistemas de IoT e indicar, para cada patrón de diseño arquitectónico, aquellos ámbitos en los que sea más viable su implementación.
- Ampliar las capacidades de la aplicación de usuario, permitiendo al mismo obtener diferentes vistas sobre el estado del sistema y

conectarse con dispositivos, no solo en una red local, sino que también a través de internet y de otras interfaces de conexión (e.g. Bluetooth, ZigBee, Serial).

- Permitir el establecimiento de comportamientos más complejos en los dispositivos IoT, durante la etapa de diseño arquitectónico del sistema, evitando la necesidad de tener que re-programar cada uno de los dispositivos manualmente.

4. FORMACION DE RECURSOS HUMANOS

Los progresos obtenidos en esta línea de investigación sirven como base para el desarrollo de tesis de posgrado, ya sea de doctorado o maestrías en Ingeniería de Software y desarrollo de trabajos finales de las carreras Licenciatura en Ciencias de la Computación, Ingeniería en Informática e Ingeniería en Computación de la Universidad Nacional de San Luis, en el marco de los Proyectos de Investigación.

5. BIBLIOGRAFÍA

[1] IEEE. Towards a Definition of the Internet of Things (IoT). 27 05 2015. https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

[2] ETSI. ETSI Technical Specification, "Machine-to-Machine Communications (M2M); M2M Service Requirements." Technical Specification. 08 2010. www.etsi.org/deliver/etsi_ts/102600_102699/102689/01.01.01_60/ts_102689v010101p.pdf

[3] M. Kranz. Internet Of Things. Construye nuevos modelos de negocio. LID Editorial, 2017.

[4] OWASP, IoT Attack Surface Areas Project, https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Attack_Surface_Areas

[5] D. Zeng, S. Guo y Z. Cheng. The Web of Things: A Survey (Invited Paper). 2011. http://www.jocm.us/index.php?m=content&c=index&a=show&catid=50&id=134

[6] IETF, The Internet of Things - Concept and Problem Statement, 2010. https://www.ietf.org/archive/id/draft-lee-iot-problem-statement-05.txt

[7] A. Bassi, M. Bauer, M. Fiedler, T. Kramp, R. v. Kranenburg, S. Lange y S. Messner. Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model. *SpringerOpen.* 2013.

[8] CERP-IoT. Visions and Challenges for Realising the Internet of Things. 2010. http://www.internet-of-things-research.eu/pdf/IoT_Clusterbook_March_2010.pdf

[9] H. Ren, H. Li, Y. Dai, K. Yang y X. Lin. Querying in Internet of Things with Privacy Preserving: Challenges, Solutions and Opportunities. 13 03 2018. http://ieeexplore.ieee.org/document/8315210/

[10] T. Choudhury, A. Gupta, S. Pradhan, P. Kumar y Y. S. Rathore. Privacy and Security of Cloud-Based Internet of Things (IoT). 28 10 2017. http://ieeexplore.ieee.org/document/8307328/

[11] M. El-hajj, M. Chamoun, A. Fadlallah y A. Serhrouchni. Taxonomy of authentication techniques in Internet of Things (IoT). 12 2017. http://ieeexplore.ieee.org/document/8305419/

[12] J. Singh, T. Pasquier, J. Bacon, H. Ko y D. Eyers. Twenty Security Considerations for Cloud-Supported Internet of Things. *IEEE Internet of Things Journal*. 2015.

[13] A. Zanella, N. Bui, A. Castellani, L. Vangelista, M. Zorzi. Internet of Things for Smart Cities. *IEEE Internet of Things Journal*. 02 2014. http://ieeexplore.ieee.org/document/6740844/

[14] S. Pérez, J. L. Hernández-Ramos, S. N. Matheu-García, D. Rotondi, A. F. Skarmeta, L. Straniero y D. Pedone. A lightweight and flexible encryption scheme to protect sensitive data in Smart Building scenarios. 02 2018. http://ieeexplore.ieee.org/document/8279412/

[15] S. Pérez, P.Gaur, M. P. Tahiliani. Operating Systems for IoT Devices: A Critical Survey. *2015 IEEE Region 10 Symposium*. 05 2015. http://ieeexplore.ieee.org/document/7166231/