SOLUCIONES DE IOT: ÁMBITOS DE APLICACIÓN Y DESAFÍOS

Sebastián U. Flores, Mario Berón, Daniel Riesco
Departamento de Informática - Facultad de Ciencias Físico Matemáticas y Naturales
Universidad Nacional de San Luis - Ejército de Los Andes 950 - San Luis - Argentina
s.flores@outlook.com.ar, { mberon, driesco }@unsl.edu.ar

RESUMEN

El Internet of Things involucra un conjunto heterogéneo de tecnologías, posee diferentes ámbitos de aplicación y un gran número de riesgos asociados. Es por ello que se debe analizar minuciosamente cada componente de las soluciones a crear. Un componente esencial a tener en cuenta son las personas. Estas interactúan con el sistema, a veces de forma voluntaria y otras, desconociendo su presencia. Diferentes regiones geopolíticas han llevado adelante legislaciones de diferentes características, con el fin de proteger a las personas frente a vulneraciones de su privacidad, o a los posibles riesgos de seguridad físicos asociados a la interacción con soluciones tecnológicas, sea que estas involucren IoT o que no lo hagan. Un sistema de IoT Industrial posee diferentes riesgos y legislaciones a los que posee un sistema hogareño para el control de electrodomésticos, o una red de producción y distribución eléctrica inteligente.

No obstante, los riesgos van más allá de su relación con las personas. Están también relacionados con el negocio, y la posibilidad de que se detenga el funcionamiento del sistema, o que se tomen decisiones incorrectas a partir de la captura de datos erróneos.

Este artículo pretende presentar el estado del arte del IoT y abordar algunos de sus desafíos más importantes en la actualidad.

Palabras clave: *IoT, Dispositivo, Nube, Escalabilidad, Seguridad, Privacidad, Confiabilidad, Arquitectura, Internet.*

CONTEXTO

La presente línea de investigación se enmarca en el proyecto de investigación denominado *"Ingeniería del Software: Estrategias de Desarrollo, Mantenimiento y Migración de Sistemas en la Nube"*. El proyecto, a su vez, es un *Proyecto de Investigación Consolidado - PROICO*, y posee el código *03-2020*. 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.

1. INTRODUCCIÓN

De acuerdo con Oracle [1], el Internet de las cosas (IoT) describe la red de objetos físicos ("cosas") que llevan incorporados sensores, software y otras tecnologías con el fin de conectarse e intercambiar datos con otros dispositivos y sistemas a través de Internet.

A grandes rasgos, podrían identificarse varios ámbitos de aplicación de tecnologías IoT [2]:

- Hogares conectados. Los dispositivos de IoT pertenecientes a este ámbito incluyen una amplia gama de electrodomésticos creados con un enfoque de *diseño orientado al usuario* [3, 4], que permite analizar el comportamiento de este último y adaptarse a sus necesidades, para mejorar la experiencia de uso y la utilidad. Este ámbito también incluye dispositivos para el incremento de la seguridad hogareña, como sensores de gas/humo, cerraduras inteligentes y alarmas, entre otros.
- Vehículos conectados. Este ámbito todavía se encuentra en etapas tempranas, e incluye, entre otros beneficios, la posibilidad de formar una red de vehículos conectados a Internet que puedan comunicarse entre sí para realizar optimizaciones en el tráfico e incrementar la seguridad de los pasajeros.
- Ciudades inteligentes. Este ámbito

incluye la posibilidad de instalar sensores en diferentes partes de una ciudad, tanto en ámbitos públicos como privados, para tener más información que ayude a mejorar los servicios públicos, la calidad del aire, disminuir el ruido ambiental, optimizar el mantenimiento de los sistemas de iluminación y carreteras, detectar fugas de cañerías de agua potable, entre otros.

- La industria. Este ámbito es conocido como Internet Industrial de las Cosas (IIoT), y refiere al uso de dispositivos para optimizar e incrementar la seguridad en fábricas, servicios de logística, venta minorista, sistemas de producción de energía, entre otros.

En los últimos años, se produjeron grandes avances tecnológicos que propiciaron el surgimiento y masificación del IoT. Algunos de estos avances se presentan a continuación:

- Disminución de los costos en sensores de buena calidad, y en chips de alta potencia.
- Grandes progresos en los medios de comunicación, que incrementaron su ancho de banda y disminuyeron, tanto su latencia como sus costos, a nivel mundial.
- Expansión y perfeccionamiento de las plataformas en la nube para el almacenamiento y procesamiento de información.
- Avances en las tecnologías de análisis de datos y aprendizaje automático.
- Incremento de la accesibilidad a la tecnología, a partir de la expansión de inteligencias artificiales conversacionales y dispositivos móviles.

Cada sistema de IoT, dependiendo del ámbito y de las necesidades de negocio, estará conformado por diferentes componentes. No obstante, los siguientes componentes podrían considerarse comunes a la mayor parte de los sistemas de IoT [2]:

- Dispositivos de IoT. Son dispositivos tecnológicos conformados por sensores, actuadores, sistemas de conectividad y microcontroladores, cuyo fin es la recopilación de datos del entorno, de los usuarios o de los patrones de uso; la comunicación de los datos recopilados a través de Internet; y la ejecución de acciones para transformar el ambiente físico donde se encuentran, por medio de sus actuadores.
- Servidores de almacenamiento y cómputo. Se encargan de integrar los datos publicados por los dispositivos IoT, almacenarlos, analizarlos por medio de aprendizaje automático y otras tecnologías, y tomar decisiones sobre los mismos. Estas decisiones incluyen informar a administradores de la solución o solicitar a los dispositivos la ejecución de diferentes acciones inteligentes. En su mayoría, se encuentran desplegados en la nube, por lo que cuentan con capacidades de almacenamiento y cómputo prácticamente sin límites.
- Puertas de enlace. Existen diversos casos en que los dispositivos no pueden comunicarse directamente con los servidores, por lo que se utilizan puertas de enlace, que son puntos de conexión que actúan como intermediarios entre los dispositivos y los servidores.
- Aplicaciones de usuario. Son aplicaciones de software que poseen interfaces visuales por medio de las cuales los diferentes usuarios de la solución IoT pueden visualizar los datos obtenidos por los dispositivos, controlar el estado de conexión, modificar configuraciones de la solución y solicitar la ejecución de acciones a los dispositivos.
- Computación de borde. Es un conjunto de tecnologías que permite dotar a los dispositivos de la capacidad de realizar un análisis y procesamiento sobre los datos obtenidos por medio de sus sensores, para tomar decisiones más rápidamente, evitando una dependencia total de los servidores.

En base a los párrafos anteriores, puede notarse que el espectro del IoT es muy amplio y que, si bien existen grandes avances, debe tenerse en cuenta una amplia variedad de factores al momento de diseñar e implementar un sistema de IoT [5, 6, 7]:

- Seguridad. Este es un factor muy importante que incluye múltiples facetas. En primer lugar, se encuentra la protección de datos en tránsito, que incluye a diferentes protocolos de comunicación entre los componentes del sistema, y diferentes formas de encriptación de los datos antes de ser transmitidos. En segundo lugar, la protección de datos en reposo incluye diferentes metodologías y algoritmos de encriptación para el almacenamiento seguro de los datos, una vez transmitidos hacia un servidor. En tercer lugar, la seguridad del hardware de los dispositivos es aquella que impide a personas sin autorización modificar los dispositivos, o bien, extraer y analizar los datos almacenados en ellos y su código fuente. En caso de usarse puertas de enlace, también deben incluirse medidas de seguridad en las mismas, ya que estas interactúan con los dispositivos y con los servidores. Adicionalmente, la seguridad debe implementarse en los servidores, para protegerlos de diferentes ataques maliciosos, como los ataques de denegación de servicio (DDoS). Para concluir, deben incluirse protecciones de seguridad complementarias para las aplicaciones de usuario, como la autenticación multifactor y la autenticación sin contraseña [8].

- Privacidad. Dependiendo del entorno en donde se desplieguen los sistemas de IoT, podrían verse involucradas diferentes personas en las mediciones de los sensores, y muchas de ellas podrían desconocer la existencia de dichos sistemas, o bien, desconocer la clase de información que estos extraen y los potenciales riesgos asociados a las vulneraciones de seguridad. Es por ello que, sumado a las protecciones de seguridad establecidas, debe minimizarse (y de ser posible, evitarse) el almacenamiento de Información de Identificación Personal (PII) [9, 10]. Por otra parte, debe informarse claramente a todas las personas que puedan interactuar con el sistema de IoT, sobre los fines del sistema y los datos extraídos, además de solicitar su consentimiento, tal y como se ha establecido en diferentes legislaciones alrededor del mundo.

- Restricciones legales. Como se mencionó anteriormente, existen diferentes legislaciones alrededor del mundo, asociadas a la privacidad, la localidad, la pertenencia y los medios habilitados para la extracción, almacenamiento y procesamiento de los datos [11, 12, 13].

- Confiabilidad. Las soluciones IoT a menudo se implementan a gran escala y, pueden funcionar en redes poco seguras o de mala calidad, con una alta exposición a condiciones ambientales adversas, que podrían afectar los requisitos establecidos en su diseño inicial. No obstante, es fundamental que la solución funcione correctamente en los momentos críticos. Es muy importante que los sensores aporten datos confiables, para evitar que se tomen decisiones erróneas. Incluso, los actuadores deben funcionar correctamente, para que pueda actuarse de la manera adecuada y en el momento que se lo necesita. Por lo mencionado anteriormente, es esencial diseñar la arquitectura de IoT con la disponibilidad y resistencia en mente, realizando una cuidadosa selección del hardware de los dispositivos, los protocolos, los servicios en la nube y los medios de conexión. También debe considerarse la posibilidad de tener redundancia en los sectores críticos de la solución, para reducir los puntos únicos de falla que afecten al sistema en su totalidad.

- Resistencia al ambiente. Dependiendo del ámbito, los dispositivos de IoT podrían estar expuestos a diferentes condiciones ambientales, como cambios de temperatura, lluvia, humedad, polvo, ruido eléctrico, inconsistencias en el suministro eléctrico o manipulación errónea por parte de los usuarios.

- Escalabilidad. Un sistema de IoT podría crecer con el tiempo de forma horizontal (si se agregan más dispositivos de un mismo tipo) o vertical (si se incluyen dispositivos diferentes). Es así que la arquitectura del sistema debe planificarse adecuadamente, buscando prever estos posibles cambios en la escala del sistema, y teniendo en cuenta el incremento en los costos, en la complejidad de la infraestructura

y en la cantidad de mensajes transmitidos.

- Flexibilidad. Las soluciones de IoT se caracterizan por la integración de componentes propios o creados por terceros, los cuales podrían utilizar diferentes protocolos de comunicación, tecnologías de hardware y software, o tener diferentes requisitos de infraestructura y mantenimiento. A su vez, pueden escalar notablemente de acuerdo con cambios en los requisitos del usuario final o a la detección de puntos de mejora. La flexibilidad aborda la capacidad de la solución de adaptarse a diferentes necesidades en diferentes momentos del tiempo.

- Eficiencia energética. Los dispositivos podrían ser desplegados en entornos donde sea difícil o costoso acceder al suministro eléctrico, por lo que deberían tener un bajo consumo energético. Esto trae otras implicancias como la selección de hardware de menor potencia, el uso de protocolos de comunicación más ligeros (y quizás, menos seguros) o la necesidad de utilizar energías renovables.

- Conectividad. Dependiendo de los riesgos de los procesos, podría requerirse una menor latencia en las comunicaciones, para poder tomar decisiones en menor tiempo. En ámbitos controlados como los industriales, es posible establecer las configuraciones necesarias de conectividad de sistemas y dispositivos locales. En ámbitos no controlados, como aquellos correspondientes a instalaciones de consumidores finales, sistemas de logística o sistemas desplegados en zonas rurales, es muy probable que el nivel de conexión se vea afectado por condiciones climáticas o disponibilidad de proveedores de conexión locales. Es por ello que los sistemas de IoT deben estar preparados para funcionar correctamente, a pesar de tener largos períodos sin conexión. Otra alternativa es realizar un despliegue de sistemas de conexión propios, como la creación de redes LoRaWAN [14].

- Presupuesto. En todos los factores mencionados antes, los costos son una variable común que influye en la selección de las configuraciones del sistema de IoT. En la medida que se busque incrementar la seguridad, mejorar la latencia o escalar el sistema, los costos se verán notablemente incrementados, tanto en los dispositivos de IoT como en el resto de la infraestructura utilizada para las comunicaciones, almacenamiento y procesamiento de datos. Debe analizarse a detalle los requisitos de negocio, los riesgos asociados al sistema y la posibilidad de que este cambie con el tiempo, para seleccionar los componentes a utilizar y conformar el presupuesto.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

Para diseñar una solución IoT, es imprescindible identificar cada uno de los problemas involucrados y atacarlos con la mejor tecnología posible, comprendiendo las limitaciones inherentes al proyecto y a factores externos.

Con el fin de facilitar la búsqueda de soluciones óptimas a los problemas que se presenten en el diseño de una solución de IoT escalable y segura, esta línea de investigación propone:

- Investigar posibles soluciones a los desafíos presentados en la introducción.
- Estudiar las legislaciones y la matriz productiva nacional y regional, para determinar posibles ámbitos de aplicación de soluciones IoT.

3. RESULTADOS OBTENIDOS/ESPERADOS

Realizar informes que detallen el estado del IoT a nivel nacional y regional, en relación con el estado en otras regiones del mundo.

Realizar propuestas de soluciones a los diferentes desafíos mencionados en la Introducción, poniendo énfasis en aquellas con mayor viabilidad a nivel nacional y regional.

Implementar, o colaborar en la implementación de soluciones de IoT reales.

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 mencionados en la Sección *Contexto*.

5. BIBLIOGRAFÍA

[1] Oracle, «¿Qué es el IoT?,» [En línea]. Available: https://www.oracle.com/es/internet-of-things/what-is-iot/.

[2] Amazon, «¿Qué es el IoT?,» [En línea]. Available: https://aws.amazon.com/es/what-is/iot/.

[3] M. Mezzenzana, «Internet-of-Things as an enabling factor for user-centered service engineering.,» 2019. [En línea]. Available: https://www.researchgate.net/publication/360256759_Internet-of-Things_as_an_enabling_factor_for_user-centered_service_engineering.

[4] ThingsCon, «User Centred IoT-Design,» 12 06 2017. [En línea]. Available: https://medium.com/the-state-of-responsible-internet-of-things-iot/andreakrajewski-aff52af1e065.

[5] Microsoft, «IoT Overview,» [En línea]. Available: https://learn.microsoft.com/es-es/azure/architecture/framework/iot/iot-overview.

[6] Microsoft, «IoT Reliability,» [En línea]. Available: https://learn.microsoft.com/es-es/azure/architecture/framework/iot/iot-reliability.

[7] S. N. C. Z. S. e. a. Moore, «IoT reliability: a review leading to 5 key research directions,» 2020. [En línea]. Available: https://doi.org/10.1007/s42486-020-00037-z.

[8] Entrust, «¿Qué es la Autenticación Multifactor (MFA)?,» [En línea]. Available: https://www.entrust.com/es/resources/faq/what-is-multi-factor-authentication-mfa.

[9] Investopedia, «What Is Personally Identifiable Information (PII)? Types and Examples,» [En línea]. Available: https://www.investopedia.com/terms/p/personally-identifiable-information-pii.asp.

[10] V. J. Guareteguá, «Información de Identificación Personal (PII) / Personally Identifiable Information (PII),» 2020. [En línea]. Available: https://www.linkedin.com/pulse/informaci%C3%B3n-de-identificaci%C3%B3n-personal-pii-personally-javier/?originalSubdomain=es.

[11] European Union, «General Data Protection Regulation,» [En línea]. Available: https://gdpr-info.eu/.

[12] Gobierno Nacional de la República Argentina, «Ley 25.326 de la Protección de los Datos Personales,» 04 10 2000. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm.

[13] State of California Department of Justice, «California Consumer Privacy Act,» 02 2023. [En línea]. Available: https://www.oag.ca.gov/privacy/ccpa.

[14] LoRa Alliance, «What is LoRaWAN® Specification,» [En línea]. Available: https://lora-alliance.org/about-lorawan/.