Ciencias de la Información 396 (2017) 72–82

Listas de contenidos disponibles enCiencia Directa

Ciencias de la información

revista Página de inicio:www.elsevier.com/locate/ins

Modelado de dinámicas de confianza en Internet de las cosas

Carmen Fernández-Gago*, Francisco Moyano, Javier López

Laboratorio de Redes, Información y Seguridad Informática, Universidad de Málaga, 29071 Málaga, España

información del artículo

Historia del artículo:
Recibido el 16 de noviembre de 2015 Revisado el 1 de diciembre de 2016 Aceptado el 15 de febrero de 2017 Disponible en línea el 17 de febrero de 2017

Palabras clave:
Confianza
Internet de las Cosas
Marco dinámico

abstracto

El Internet de las Cosas (IoT) es un paradigma basado en la interconexión de objetos cotidianos. Se espera que las "cosas" involucradas en el paradigma de IoT tengan que interactuar entre sí, a menudo en condiciones inciertas. Por lo tanto, es de suma importancia para el éxito de la IoT que existan mecanismos que ayuden a superar la falta de certeza. La confianza puede ayudar a lograr este objetivo. En este documento, presentamos un marco que ayuda a los desarrolladores a incluir la confianza en escenarios de IoT. Este marco tiene en cuenta los requisitos de confianza, privacidad e identidad, así como otros requisitos funcionales derivados de los escenarios de IoT para proporcionar los diferentes servicios que permitan la inclusión de la confianza en el IoT.

1. Introducción

El Internet de las Cosas (IoT) es un paradigma basado en la interconexión de objetos cotidianos. Según el informe Gartner de 2013[3], se espera que 26 mil millones de objetos estén conectados en IoT para 2020. Desde una perspectiva económica, el mismo informe también destaca que se espera que IoT genere 1,9 billones de dólares a partir de la producción de productos y proveedores de servicios de IoT, lo que se traducirá en crecimiento económico y empleo. Al mismo tiempo, la cantidad de datos gestionados en IoT hace necesario mirar la perspectiva centrada en los datos.[24]y considere las implicaciones de privacidad que esto podría generar. Las ventajas que aporta la IoT podrían verse seriamente amenazadas si la recepción por parte de la sociedad es negativa. Esta podría ser una posibilidad si los ciudadanos, las empresas y las administraciones sienten que no pueden confiar en el IoT. Los usuarios son cada vez más conscientes de la importancia de proteger su información privada[2,14], y las empresas se están dando cuenta cada vez más de que una estrategia de seguridad incorrecta puede provocar importantes pérdidas económicas y de reputación y, en última instancia, la quiebra.[1]El informe de Gartner de 2014 destaca que las empresas se han dado cuenta de ello y, como resultado, en 2014 aumentaron sus inversiones en seguridad en alrededor de un 8%.[1]. Pero incluso si los sistemas de IoT son realmente seguros, la sociedad puede mostrarse reacia a utilizarlos si no se abordan adecuadamente las preocupaciones sobre la confianza.

Es un hecho que las cosas tendrán que interactuar para generar valor empresarial. Las interacciones a menudo tendrán que ocurrir en condiciones inciertas. Tener mecanismos implementados que ayuden a las "cosas" involucradas en los escenarios de IoT a superar la falta de certeza se vuelve de suma importancia. Los mecanismos de seguridad tradicionales no son suficientes; sin embargo, los sistemas de gestión de confianza pueden ayudar en estos casos. Proporcionan una mayor flexibilidad que los mecanismos de seguridad tradicionales, facilitando el proceso de toma de decisiones. Al final, diseñar estos problemas de confianza en los servicios y sistemas de IoT debe ser un objetivo principal para garantizar la adopción exitosa del paradigma de IoT. Hay varios desafíos relacionados que deben superarse. En primer lugar, desde un punto de vista técnico, la propia IoT plantea nuevos desafíos en materia de seguridad y confianza, dado que nuevos modelos de interacción,

* Autor correspondiente.
*Correos electrónicos:*mcgago@lcc.uma.es (C. Fernández-Gago),moyano@lcc.uma.es (F. Moyano),jlm@lcc.uma.es (J. López).

[1] http://www.pcworld.com/article/2046300/hackers-put-a-bulls-eye-on-small-business.html.

http://dx.doi.org/10.1016/j.ins.2017.02.039 0020-0255/

como Machine to Machine (M2M), están ganando terreno. En segundo lugar, la naturaleza de los escenarios de IoT los hace altamente dinámicos y heterogéneos, ya que las cosas entran y salen constantemente de los entornos de IoT. Por tanto, los sistemas diseñados para entornos de IoT deberían reflejar estos desafíos y deberían tener en cuenta lo siguiente:

- *Interoperabilidad*. Dispositivos con diferentes capacidades, de diferentes fabricantes y, probablemente, adheridos a diferentes estándares, deben poder comunicarse. Además, los diferentes sistemas de gestión de confianza que pueden coexistir en entornos de IoT deben ser interoperables y capaces de intercambiar información de otros sistemas de confianza.
- *Dinamismo*. La dinámica de los sistemas de IoT, donde nuevos dispositivos y servicios pueden entrar y salir del sistema a intervalos impredecibles, implica que los sistemas de gestión de confianza también deben evolucionar con los sistemas.
- *Investigación fragmentada*. Las comunidades de investigación están abordando las cuestiones anteriores de forma aislada. Este también es el caso en otras áreas de investigación importantes que deben respaldar la confianza en los sistemas de IoT, como la gestión de identidad y la privacidad. Se necesita un enfoque holístico.

En resumen, la complejidad de las tecnologías de IoT y la fragmentación de la investigación de IoT son dos obstáculos que impiden a los desarrolladores obtener los conocimientos adecuados para diseñar e implementar sistemas de IoT completos y confiables. En consecuencia, podemos esperar que los sistemas construidos se vean afectados y que los usuarios finales no queden satisfechos. Abogamos por que mejores herramientas puedan crear mejores productos. Presentamos un marco que comprende un conjunto de herramientas y servicios que los diseñadores y desarrolladores pueden utilizar para integrar cuestiones de confianza en los sistemas de IoT. El marco está dirigido a diseñadores y desarrolladores, pero sus beneficios se reflejarán en los usuarios finales de los sistemas de IoT, quienes se sentirán más seguros acerca de su adopción, ya que eventualmente tendrán una experiencia de mejor calidad.

El documento está estructurado de la siguiente manera.Sección 2revisa el trabajo existente sobre gestión de confianza para IoT.Seccion 3 profundiza en el problema de la confianza y el IoT, ySección 4describe nuestra propuesta de una arquitectura para incluir la confianza en los sistemas de IoT.Sección 5demuestra cómo se puede aplicar el marco en un escenario de IoT. Finalmente,Sección 6concluye el artículo y describe el trabajo futuro.

2. Trabajo relacionado

El concepto de confianza en informática se toma del concepto en entornos sociológicos, psicológicos y económicos. La definición de confianza no es única. Puede variar según el contexto en el que se vaya a utilizar y con qué finalidad. A pesar de considerarse de suma importancia al considerar la seguridad de los sistemas, aún no se ha proporcionado una definición estándar de confianza. Sin embargo, está ampliamente aceptado que la confianza podría ayudar en los procesos de toma de decisiones, como los involucrados en los esquemas de control de acceso.

Los sistemas de gestión de confianza surgieron por primera vez en la literatura como una forma de resolver problemas de control de acceso y unificar la autenticación y autorización en sistemas distribuidos.[8]. Los orígenes de la confianza computacional se remontan a los años noventa, cuando el trabajo en[15]analizaron factores sociales y psicológicos que influyen en la confianza y replicaron este concepto en un entorno computacional. Desde entonces, se han desarrollado muchos sistemas diferentes de gestión de confianza para diferentes aplicaciones. Un modelo de confianza comprende el conjunto de reglas y lenguajes necesarios para forjar la confianza entre entidades de forma automática o semiautomática.

La heterogeneidad en el número de sistemas de gestión de confianza a menudo genera confusión, ya que fácilmente se podrían perder los conceptos más relevantes que sustentan estos modelos de confianza. Por concepto de confianza o concepto relacionado con la confianza nos referimos a cualquier noción que tenga una alta relevancia de acuerdo con la frecuencia con la que surge la noción en los modelos de confianza existentes. Al analizar estos conceptos de confianza, Moyano et al.[17]diseñó un modelo conceptual para la confianza que sirve como base para un marco de desarrollo que respalda la adaptación de modelos heterogéneos de confianza y reputación.[19]. En este enfoque, los autores distinguieron dos tipos de modelos de confianza:

- *Modelos de decisión*. La gestión de la confianza tiene su origen en estos modelos[8]. Su objetivo es flexibilizar las decisiones de control de acceso, simplificando el proceso de autenticación y autorización de dos pasos en una decisión de confianza de un solo paso. Los modelos de políticas y los modelos de negociación entran en esta categoría. Se basan en las nociones de políticas y credenciales, restringiendo el acceso a los recursos mediante políticas que especifican qué credenciales se requieren para acceder a ellos.
- *Modelos de evaluación*. A estos modelos se les suele denominar confianza computacional, la cual tiene su origen en el trabajo en[15]. Su intención es evaluar la confiabilidad (u otro atributo similar) de una entidad midiendo ciertos factores que influyen en la confianza. Dos subtipos de modelos en esta categoría son los modelos de propagación, que difunden información de confianza a lo largo de cadenas de confianza, y los modelos de reputación, en los que las entidades utilizan las opiniones de otros sobre una entidad determinada para evaluar su confianza en esta última.

Se están haciendo muy pocos esfuerzos para diseñar sistemas de gestión de confianza para IoT. Se considera un entorno de IoT específico donde las "cosas" son sólo sensores inalámbricos.[9]. La solución de gestión de confianza en este caso sólo resuelve el problema del reenvío de paquetes. Por lo tanto, este enfoque no aborda la heterogeneidad a la que apunta el paradigma de IoT. Bao y Chen[6]diseñó un protocolo de gestión de confianza escalable para IoT que tiene en cuenta las relaciones sociales y utiliza propiedades como la honestidad, la cooperación y el interés de la comunidad para evaluar la confianza. El protocolo se distribuye y los nodos actualizan la confianza solo para los nodos que les interesan o con los que interactúan. Las actualizaciones se realizan a través de observaciones directas o recomendaciones indirectas. Basado en este modelo, los mismos autores propusieron un protocolo dinámico de gestión de confianza para que IoT se ocupe de nodos que se comportan mal o de comportamientos que pueden cambiar dinámicamente.[5]. Un punto de vista distinto

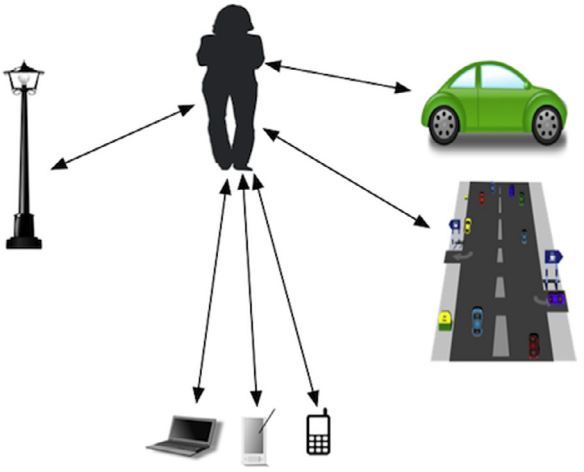

Figura 1. Un contexto para un usuario.

sobre cómo interactúan las cosas en el paradigma de IoT se presenta en[4]. En este artículo los autores consideraron que los objetos en un escenario de IoT conforman una red social donde establecen relaciones de confianza social. Introdujeron una arquitectura para el Internet social de las cosas (SIoT). La confianza no se considera explícitamente, pero proponen un método para determinar nodos confiables en este entorno socializado. el trabajo en[25]propuso un sistema centralizado de gestión de confianza para IoT que tiene como objetivo gestionar la cooperación entre nodos con diferentes capacidades de recursos. El modelo asignó valores de confianza a los nodos cooperantes según diferentes contextos. Ninguno de estos enfoques considera la inclusión de la confianza en entornos de IoT de forma dinámica, considerándola en las primeras etapas del diseño de servicios de IoT, como proponemos en este artículo. Para abordar la dinámica en IoT, introducimos el concepto de trust@run.time (verSeccion 3). Existe un interés creciente en considerar nociones de confianza en sistemas autoadaptativos para aprovechar las decisiones de reconfiguración, especialmente en las áreas de multiagente.[13,26], basado en componentes[12,27]y sistemas orientados a servicios[11,23]. Estos enfoques abogan por el uso de la confianza y la reputación para desarrollar sistemas altamente dinámicos y sensibles a la seguridad, lo que justifica su exploración en casos de uso más amplios, como los presentes en el IoT.

3. Desafíos para integrar la confianza en el Internet de las Cosas

Se espera que las "cosas" en entornos de IoT interactúen entre sí. En la mayoría de los casos, las interacciones tendrán que ocurrir incluso si no hay suficiente información sobre las cosas para establecerlas. La información disponible sobre una cosa en una aplicación puede provenir no sólo de su comportamiento en las interacciones de otros con ella, sino también de la información que puede proporcionarse debido a todas las "cosas" que la rodean. Nuestra suposición es que las cosas no son sólo entidades físicas sino más bien el conjunto completo de "cosas" que interactúan con ellas; esto es lo que llamamos el*contexto*.Figura 1ilustra un escenario tradicional de IoT donde el contexto de la persona en la figura (una cosa también según nuestra suposición) está representado por los objetos a los que apuntan las flechas.

Hay dos desafíos principales que debemos abordar si queremos brindar una solución holística para la gestión de confianza en IoT: la interoperabilidad y la dinámica/evolución. La interoperabilidad es un problema que se deriva directamente del hecho de afrontar la heterogeneidad del IoT. Diferentes cosas tendrán sus propios sistemas de gestión de confianza que tendrán que intercambiar información con otros y, por tanto, diferentes sistemas de gestión de confianza que podrán coexistir. El marco propuesto permitirá que los modelos de confianza utilicen diferentes lenguajes o diferentes formas de determinar la confianza para obtener información de confianza común para todos.

En términos de evolución del sistema, existe una relación bidireccional entre los sistemas de IoT y sus sistemas de gestión de confianza. Por un lado, dado que los sistemas de IoT y sus contextos son dinámicos, los sistemas subyacentes de gestión de la confianza deben cambiar para satisfacer las preocupaciones más recientes sobre la confianza. Por ejemplo, pueden aparecer nuevas fuentes de información relacionada con la confianza. Por otro lado, los valores de confianza y reputación pueden provocar cambios en los sistemas de IoT. Si la relación de confianza entre dos "cosas" cae por debajo de cierto umbral, o la reputación de una "cosa" es demasiado baja, es posible que se requieran cambios en el sistema para mantener un nivel tolerable de confianza. Hasta ahora, la dinámica de tales escenarios y la construcción de sistemas de gestión de confianza que cambian en tiempo de ejecución han quedado fuera de la literatura. Proponemos considerar ' trust@run.time ', que ha sido desarrollado a partir del concepto de models@run.time. [7]. Este término se refiere a mantener un modelo abstracto del sistema ejecutor de tal manera que ambos estén siempre sincronizados. Esto lleva la idea de reflexión un paso más allá, ya que podemos razonar sobre el sistema en ejecución en términos del modelo. Esta idea ha tenido una gran aceptación entre la comunidad autoadaptativa, ya que propone que los cambios en el modelo se reflejen automáticamente en el sistema en ejecución, fomentando una evolución rápida y fluida. Defendemos esto como un paso natural hacia el soporte de sistemas de IoT altamente dinámicos, porque pueden ser necesarios diferentes modelos de confianza y reputación dependiendo de los contextos de los sistemas a lo largo de su vida útil. La idea de

trust@run.time fue propuesto por primera vez por Moyano[dieciséis], pero existe un interés creciente en considerar nociones de confianza en sistemas autoadaptativos para aprovechar las decisiones de reconfiguración.

4. Incluir la confianza en el IoT

El marco que proponemos tiene como objetivo ayudar a los desarrolladores a agregar confianza o reputación a los sistemas de IoT. En lugar de tener que implementar cada modelo de confianza desde cero, nuestro marco facilita el trabajo de los desarrolladores proporcionándoles técnicas y orientación para reutilizar características comunes de otros modelos de confianza y seguir ciertos pasos para llevar a cabo la implementación.

Los requisitos de confianza y reputación no son los únicos que afectan los escenarios de IoT. La gestión de la privacidad y la identidad, así como otros requisitos no funcionales, serán de suma importancia en la construcción del marco. Si estamos interesados en desarrollar un marco en el que estén presentes diferentes sistemas de gestión de confianza para IoT, debemos considerar aspectos de la gestión de identidades. Es particularmente crucial definir adecuadamente la identidad de las "cosas". Su identidad podría estar determinada por su contexto (el conjunto de cosas que están conectadas con el usuario para un propósito específico en un momento dado). Puede que no sea suficiente, o incluso aconsejable, que las cosas se identifiquen proporcionando algún tipo de identificación, por ejemplo, un login. La identidad de una cosa puede variar según el contexto donde se sitúa. La privacidad es el otro pilar importante a la hora de modelar la confianza. Existe una relación directa entre ellos. En algunos casos, podría ser que cuanta más información se divulgue, mayor será la precisión de la decisión basada en la confianza. A su vez, la divulgación de información plantea preocupaciones sobre la privacidad que es necesario tener en cuenta. Sin embargo, podría ser que la confianza ayude a preservar la privacidad, ya que puede usarse para evitar establecer comunicación con algo que no es de confianza.

Miremos la cosa, en este caso una persona, enFigura 1. Su identidad útil para este escenario es aquella que, en el momento en que pasa por una carretera, puede obtener u ofrecer información a las demás cosas que la rodean (farol, tarjeta, etc.). En este escenario no es relevante si es médico o abogado, por ejemplo. Estas dos características podrían ser relevantes en otros escenarios, por ejemplo, cuando se trata de las oficinas de impuestos o de seguros nacionales de su país.

Teniendo todas estas consideraciones en mente, creemos que tanto la privacidad como la identidad son propiedades que siempre deben estar presentes al diseñar sistemas de gestión de confianza y reputación.

4.1. Arquitectura

Para construir el marco para el desarrollo de sistemas de gestión de confianza para IoT, la arquitectura que proponemos se divide en cuatro capas, donde cada una de ellas se basa en los resultados de su capa inferior. Las capas son las siguientes:

- *Capa de escenarios*. Esta capa se ocupa de la identificación de escenarios de IoT. A partir de estos escenarios se identifican los diferentes contextos que pueden surgir en cada uno de ellos. Dado que la dinámica y la evolución son capturadas por los cambios en el entorno en cada momento, nuestra intención es capturar estos cambios a nivel de contexto. En esta capa sentamos las bases para un concepto clave que introducimos: el concepto de contexto de una cosa.
- *Capa de requisitos*. Los contextos identificados en la capa anterior serán la base para derivar requisitos relacionados con la gestión de identidad, privacidad y confianza en ésta. Estos requisitos se utilizarán en diferentes elementos de la capa de servicios. Podría haber varias formas de representar los requisitos. En[20]Se utiliza una extensión de UML con requisitos de confianza para representar los requisitos que pueden surgir al diseñar un modelo de confianza. Usaremos un enfoque basado en SI⋆donde una extensión de la confianza para incluir la representación de los requisitos de confianza[22]es presentado. Usaremos esta extensión para incluir requisitos de privacidad e identidad. La forma exacta en que se realizará esta extensión está fuera del alcance de este documento por razones de extensión.

- *Capa de servicios*. Los servicios aquí incluidos van desde la definición o almacenamiento de contextos, hasta la implementación de los modelos de confianza, cómo considerar la interoperabilidad o cómo se aborda la dinámica y la evolución. Dado que los modelos de confianza deben evolucionar junto con el sistema, los requisitos de confianza influyen en la dinámica. El servicio de dinámica y evolución permitirá a los desarrolladores acceder y modificar los modelos de confianza.
- Capa de marco de confianza. Esta capa es la realización y el objetivo final del marco. Incluye varios servicios que están empaquetados en un marco de desarrollo orientado al flujo de trabajo que, en última instancia, se entrega a los diseñadores y desarrolladores a través de API (interfaces de programación de aplicaciones). El marco consta de una API para desarrolladores con algunos componentes básicos que se pueden ampliar, algunos métodos que se pueden anular y archivos de configuración.

Figura 2muestra la arquitectura propuesta, construida con un enfoque ascendente.

4.2. Marco de confianza y servicios.

En esta sección, nos concentramos en la capa central del marco, que es la capa de servicios que dará como resultado el marco propuesto. Los escenarios y las capas de requisitos se utilizan como entradas para la capa de servicio. Están determinados por los diferentes casos de uso y los requisitos identificados para ellos.

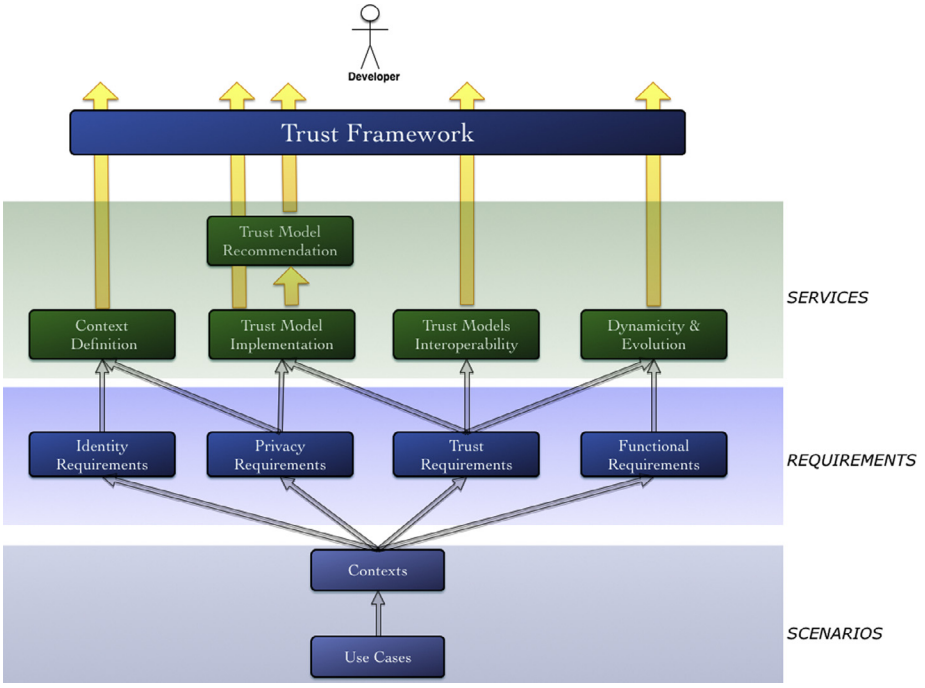

Figura 2. Arquitectura del marco de confianza para entornos IoT.

4.2.1. Definición de contexto

La dinámica de un modelo de confianza podría captarse si somos capaces de determinar los factores que influyen en la confianza en un momento dado para un propósito específico. Abogamos por que los modelos de confianza que se vayan a definir para una determinada "cosa" no dependan sólo de su comportamiento sino también de lo que llamamos la*Contexto*o cosas a su alrededor. Los contextos se refieren a un momento específico en el tiempo. Así, definimos el contexto de una cosa como el conjunto de cosas que están conectadas a ella (incluyendo aquello para lo que estamos definiendo el contexto) en un momento dado y que proporcionan información para un propósito específico. Estos propósitos influyen en su comportamiento y su relación con otras cosas. Pueden ser, por ejemplo, detectar la temperatura, medir el tráfico, etc.

Debido a la heterogeneidad de los escenarios de IoT, puede haber una gran cantidad de contextos incluso para un solo caso de uso. La identificación de los diferentes contextos nos dará información sobre los requisitos que plantea el IoT, en particular, los relacionados con la identidad, la privacidad o la confianza.

El servicio de definición de contexto dependerá del conjunto de cosas (t)de un escenario dado. Para un propósito específico,*pag*, y una cosa dada (t_i), el servicio proporcionará un subconjunto de$t$en un momento específico en el tiempo,t_i. Además, el mero hecho de considerar la evolución del escenario en el tiempo puede influir en la existencia de contextos. El propósito determina el subconjunto de cosas que están conectadas at_iy hay que considerarlo. Así, por ejemplo, si el propósito es tener información sobre el estado del tráfico, es irrelevante considerar los elementos que controlan el consumo eléctrico doméstico. El servicio también contará con un repositorio de contextos que se pueden utilizar para definir nuevos contextos reutilizando los existentes. Esto facilitará la definición de modelos de confianza, ya que los actores (fideicomitente y fiduciario) no siempre tienen que definirse como nuevos y pueden reutilizarse en otros contextos.

4.2.2. Interoperabilidad entre modelos de confianza

Una de las principales características de los entornos de IoT es la variedad de cosas que están interconectadas. Esto significa que es posible que diferentes modelos de confianza tengan que interactuar incluso si son de diferentes tipos. Por tanto, sería deseable que pudieran interpretar y comprender los idiomas de los demás y sus formas de generar confianza. Se puede lograr la interoperabilidad mediante el establecimiento de asignaciones entre los modelos, que generalmente son asignaciones entre diferentes funciones matemáticas. En el caso de que los modelos que interactúan sean ambos modelos de evaluación (aquellos que calculan la confianza mediante el uso de un motor de confianza que deriva un valor concreto, como en el caso de los modelos de reputación), deberían usar las mismas escalas que los demás con los que interactúan. con, los mismos aspectos a medir o valores de confianza resultantes. Así, el mapeo a definir en estos casos será un mapeo que permita a ambos modelos utilizar las mismas escalas e interpretar los resultados de la misma manera. La correlación entre los modelos de confianza de evaluación y de decisión (basados en políticas) es una cuestión más complicada que también habrá que abordar. Dado que estos dos tipos de modelos funcionan en dominios diferentes, el problema se puede abordar estableciendo una semántica común y, a partir de este momento, definir asignaciones entre los diferentes valores de confianza de cada modelo, sea cual sea el formato. Como ejemplo de modelos de confianza muy ingenuos, describimos la siguiente situación. Imaginemos un modelo de evaluación donde los resultados de confianza

son 0, 1, 1,5 y 2. Imaginemos también un modelo de decisión muy simple donde los resultados proporcionados son*se establece la confianza* y *la confianza no está establecida*. Una forma muy sencilla de mapear estos modelos sería decir que 0 y 1 podrían significar *se establece la confianza*y 1,5 y 2 podrían significar*la confianza no está establecida*. Por tanto, el servicio de interoperabilidad debería permitir la definición precisa de estas correspondencias. La definición de los mapeos no es una cuestión fácil y no se puede generalizar ya que dependerá de los diferentes escenarios, que tienen diferentes requisitos y modelos de confianza.

4.2.3. Servicio de dinámica y evolución.

Los escenarios de IoT son intrínsecamente dinámicos y provocan cambios en el entorno y los contextos que viven en ellos. Los sistemas de gestión de confianza deben adaptarse en tiempo de ejecución como respuesta a estos cambios. Para abordar la dinámica, es necesario representar el estado actual del sistema y sus relaciones de confianza en tiempo de ejecución. Este servicio permite cambiar el sistema de acuerdo con cambios en las relaciones de confianza o valores de reputación. Una forma de abordar el problema de la dinámica es el concepto de trust@run.time (Seccion 3), donde hay una representación (un modelo) del sistema de gestión de confianza, que está sincronizado con los sistemas en ejecución reales. Esto nos permite razonar sobre el sistema y realizar cambios de alto nivel que se traducen automáticamente en cambios del sistema en ejecución.

Las funcionalidades que ofrece el servicio se pueden dividir en dos grandes áreas: trust@run.time y especificación de políticas de reconfiguración. El primero es un paradigma introducido por Moyano et al.[dieciséis], que es una evolución natural respecto a models@run.time [7]. En esencia contamos con una capa de reflexión que representa el estado del sistema y los modelos de confianza en tiempo de ejecución con modelos. Cualquier cambio en estos modelos conlleva una adaptación del sistema para cumplir con el nuevo modelo.

4.2.4. Servicio de implementación

El marco dinámico que proponemos también debería incluir directrices para que los desarrolladores implementen los modelos de confianza. Podemos utilizar el marco de implementación presentado en[16,18]. Este marco consta de varias clases que los desarrolladores pueden personalizar mediante herencia y anulando o implementando algunos de sus métodos. Estas clases utilizan el marco Kevoree.[2][10] clases como bloques de construcción fundamentales. Los desarrolladores pueden crear modelos de confianza y reputación directamente en la plataforma models@run.time proporcionada por Kevoree, que a su vez permite utilizar información de confianza y reputación para decisiones de reconfiguración en tiempo de ejecución.

4.2.5. Servicio de recomendación de modelos de confianza.

Este servicio no es estrictamente necesario para el framework pero aparece como resultado del resto de servicios y puede resultar útil para encontrar el modelo de confianza más adecuado para cada caso. En un entorno heterogéneo como el IoT, en ocasiones puede resultar muy útil elegir el modelo de confianza más adecuado a utilizar entre los diferentes disponibles para una misma cosa.

La siguiente sección proporciona más información sobre el marco al demostrar su aplicación en un escenario real.

5. Escenario de aplicación: equipos de servicio de campo

El escenario que hemos elegido para mostrar cómo el marco presentado enSección 4podría aplicarse, considera un equipo de servicio de campo (FST).[3]Existe un sistema, al que llamamos Sistema de Despacho (DS), que asigna tareas a los operadores. Este proceso de asignación requiere una decisión, y esta decisión puede estar respaldada por la confianza. El objetivo del DS es optimizar las asignaciones asignando tareas a aquellos operadores en quienes se puede confiar más para cumplirlas. Una tarea puede involucrar varios factores, incluyendo una complejidad estimada, un nivel de seguridad/riesgo, una duración estimada y el perfil profesional preferido/requerido. Asimismo, los operadores tienen varios factores que el DS puede explotar, como su perfil profesional, el total de horas trabajadas hasta ese momento, las tareas realizadas durante el día, la proximidad al lugar de la tarea, los años de experiencia y una puntuación de reputación. . La mayor parte de esta información puede obtenerse del contexto de los operadores, que consta de los dispositivos que llevan consigo, como gafas inteligentes, PDA/tabletas y relojes inteligentes. Este contexto puede cambiar dinámicamente debido a diferentes eventos: un operador olvida la PDA/tableta, un operador cambia de la PDA a un reloj inteligente, la conexión inalámbrica entre el sistema y la tableta se corta por problemas con el dispositivo, etc. Además, el operador puede necesitar un automóvil para llegar al lugar donde va a realizar la tarea; por lo tanto, el automóvil se agregaría al contexto del operador y podría proporcionar más información que el DS puede aprovechar para tomar una decisión de confianza, como la gasolina restante en el tanque (por ejemplo, el DS no puede confiar en que un operador complete una tarea si el operador no puede alcanzarlo antes de la hora de finalización). El sistema debe ser capaz de adaptarse dinámicamente a estos cambios en los contextos del operador para maximizar la información recopilada y su utilidad antes de tomar una decisión de confianza.

5.1. Caso de uso

Imagínese una empresa de gas. Un sensor ha detectado que una tubería tiene una fuga de gas e informa al Sistema de Detección de Problemas (PDS) de la ubicación del problema y su criticidad, que está configurada como alta. El PDS, consultando una base de datos de experiencias interna, estima la duración de la tarea y el perfil profesional más adecuado y envía toda esta información al DS.

[2] http://kevoree.org.

[3] http://community.dynamics.com/b/msftdynamicsblog/archive/2015/04/10/the-intelligent-service-technician-empowering-field-service-with-smartglasses.

El DS inicia sondeos con todo lo conectado a la red corporativa. El teléfono inteligente de Anne recibe una sonda y envía un *ack*. De vuelta al DS. El DS solicita más información, como la ubicación de Anne, el nombre del propietario del teléfono inteligente (es decir, Anne) y el total de horas de trabajo del día. El teléfono inteligente envía el GPS y la información de contacto de Anne al DS, pero como ignora el total de horas de trabajo, busca otros dispositivos en el mismo contexto hasta encontrar la PDA de Anne. Este último controla el total de horas de trabajo y lo envía al teléfono inteligente, que a su vez lo reenvía al DS. Dado que la ubicación de la tarea está a 20 minutos a pie, el DS envía la ubicación al coche de Anne, que también está en su contexto, y calcula si el coche tiene suficiente gasolina para llegar desde su ubicación actual hasta la ubicación de la tarea. En este caso, hay suficiente y, por tanto, el coche envía una respuesta positiva al DS. Con toda esta información, el DS calcula un valor de confianza que resulta ser el más alto de todos los operadores del entorno. Por lo tanto, el DS envía al PDA de Anne la nueva asignación de tarea, pero hay un problema de conexión y el DS la envía nuevamente, pero esta vez a una aplicación instalada en el teléfono inteligente. Aparece una nueva asignación de tarea en la aplicación que le brinda a Anne información sobre la ubicación de la tarea. Al llegar al lugar, Anne solicita más información sobre la estructura y el material de la tubería, y el sistema de visualización de tareas envía dicha información como una interfaz de visualización frontal a sus gafas inteligentes.

El mismo proceso se realiza con otro usuario, Bob. De esta forma, la compañía gasista dispondrá de información de ambos usuarios para poder decidir quién es el mejor a quien acudir y solucionar el problema de la fuga en la tubería.

5.2. Aplicación del marco

El marco que hemos introducido en Sección 4 se puede utilizar para implementar el escenario (es decir, el marco debe ser utilizado por ingenieros de software y no por la compañía de gas). Como hemos visto en Sección 4, el marco se compone de diferentes capas. En los siguientes párrafos, detallaremos cómo se puede aplicar este marco en el caso de uso presentado en Sección 5.1, capa por capa. Lo ejemplificaremos en el caso de la operadora Anne pero, como hemos comentado, el proceso será similar para cada operador en campo.

5.2.1. Capa de escenarios

La capa inferior del marco (como se muestra en Figura 2) define los casos de uso e identifica los contextos involucrados en cada uno de ellos. Para simplificar la descripción, identificaremos solo dos contextos para el caso de uso descrito anteriormente, y solo en el caso de la usuaria Anne.

En el momento inicial en el tiempo, t_0, supongamos que el contexto de la usuaria Anne comprende una PDA, un reloj inteligente y gafas inteligentes. El propósito, *pag*, consideramos es la asignación de la tarea de "atender una tubería con fuga" por parte de la empresa gasista. Así, el contexto del usuario Anne (t_0) Se define como $C_0 \equiv C_{t_0}(pag)$ y contiene los elementos PDA, reloj inteligente y gafas inteligentes. Como inferido de la definición de contexto en Sección 4, el usuario también forma parte de su propio contexto como una cosa más del conjunto.

Estas cosas en el contexto de Anne ayudarán a recopilar información sobre su proximidad a la tarea, las horas restantes que Anne puede trabajar en las tareas asignadas, la cantidad de tareas completadas y la reputación de Anne, que se actualiza mediante un modelo de reputación (dirigido por la compañía de gas) una vez que Anne haya terminado las tareas previamente asignadas.

Supongamos que en un momento diferente, Anne deja su PDA y usa un automóvil. Entonces, su contexto cambia, siendo en este caso, $C_1 \equiv C_{t_1}(pag)$ compuesto por un reloj inteligente, gafas inteligentes y un automóvil (suponiendo que el automóvil tenga conexión inalámbrica). El
La información que el contexto de Anne recopilará y proporcionará será más o menos la misma, aunque añadiendo en este caso información sobre la gasolina en el tanque necesaria para llegar al lugar de la fuga.

Se espera que este servicio mantenga registros de todos los contextos para poder reutilizarlos cuando se reciba uno nuevo. La idea es reutilizar información sobre las cosas y no tener que definirlas todas desde cero.

5.2.2. Capa de requisitos

Esta capa será la encargada de recoger los requisitos derivados de cada uno de los contextos para cada caso de uso. Como se muestra en Figura 2, los requisitos se agrupan en diferentes categorías. Sin embargo, estamos interesados en proporcionar más información sobre los requisitos de confianza, dado que el objetivo principal del marco es incluir la confianza, aunque se deben tener en cuenta los requisitos funcionales al diseñar todo el sistema. Los requisitos de privacidad e identidad también son de suma importancia, ya que consideramos que influyen en la confianza. Los requisitos funcionales están más allá del alcance de este documento.

Requisitos de identidad. Una de las principales características de nuestro marco es que se basa en la dinámica. Esta dinámica se deriva del escenario y el marco respalda la implementación de dichos escenarios dinámicos. La dinámica se refleja en las diferentes identidades que una cosa podría tener, dependiendo del contexto donde se encuentre. Debería haber un sistema de gestión de identidades que asigne una identidad que dependa del contexto a cada una de las cosas. Así, por ejemplo, la identidad del reloj inteligente que lleva Anne en $C_{t_0}(pag)$ debería ser diferente del que lleva puesto en contexto $C_{t_0}(pag)$, como pueden estar recopilando información diferente porque están capturando diferentes momentos en el tiempo.

Requisitos de privacidad. Es muy importante que la información que la empresa y Anne intercambian permanezca entre ellos y no se muestre a otro empleado. Este es el principal requisito de privacidad que prevemos para el escenario que estamos considerando.

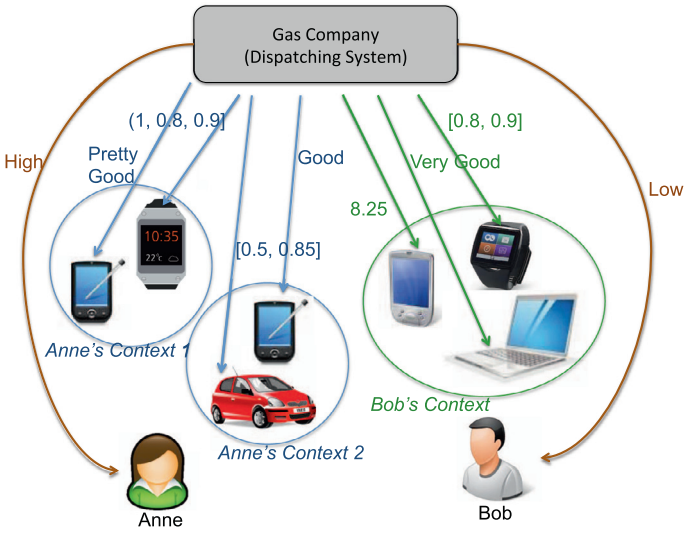

Fig. 3. Relaciones de confianza En el escenario FST, el sistema de despacho establece una relación de confianza con cada cosa, que mide la confiabilidad de la información que transmite. Estas relaciones de confianza pueden utilizar diferentes modelos de confianza y, por lo tanto, diferentes motores de confianza, que proporcionan la salida de valores de confianza en diferentes formatos, como intervalos o etiquetas cualitativas; de ahí la importancia de brindar soporte de interoperabilidad. Asimismo, el Sistema de Despacho establece relaciones de confianza con los operadores respecto de una tarea pendiente.

*Requisitos de confianza.*El objetivo final de la empresa gasista es tener toda la información disponible para tomar una decisión sobre cuál es el empleado más adecuado para solucionar una incidencia, es decir, en quién confía más la empresa para realizar la tarea. Para determinar esto, cada una de las cosas de cada uno de los contextos proporciona información a la compañía gasista. Esta información se basa en diferentes factores y es procesada por la compañía gasista, utilizando un motor de confianza para cada una de las cosas. Los motores de confianza son partes esenciales de los sistemas de gestión de confianza de las cosas. Consideramos que existe una relación de confianza entre cada cosa y la empresa que la maneja mediante un modelo de gestión de confianza para cada una de ellas. Estos modelos de confianza ayudan a determinar la confiabilidad de la información que la cosa pasa a la empresa. Por tanto, otro requisito de confianza es cómo se establece la relación entre la cosa y la empresa. Esta relación debe depender de diferentes factores que la empresa establezca, por ejemplo, si se trata de medir distancia hasta el punto de la tarea, la empresa debe considerar qué tan precisa fue esa distancia en otras ocasiones. Otros ejemplos incluyen la frecuencia con la que se tuvieron que arreglar las cosas en el pasado, el momento de la última supervisión, si el firmware o el sistema operativo de la cosa tiene alguna certificación de seguridad, etc. Todas las relaciones de confianza en el sistema se representan enFig. 3. Esta figura muestra el escenario descrito enSección 5.1con dos contextos para Anne, en dos momentos diferentes en el tiempo. También describe un contexto para Bob.

La empresa también contará con un sistema de reputación que evaluará el desempeño de Anne con respecto a las tareas que le han sido asignadas. Por lo tanto, debe haber una manera de proporcionar una*posteriormente*comentarios sobre cómo se desempeñó Anne. Esta retroalimentación puede ser de sus supervisores o de los propios sensores una vez que miden si la tubería ha sido completamente reparada o no. Este valor de reputación será otro insumo de los motores de confianza para el proceso de toma de decisiones. Así, la decisión final de confianza se tomará considerando y combinando los valores obtenidos de los diferentes motores de confianza antes mencionados y del sistema de reputación.

5.2.3. Capa de servicios

Esta es la capa donde residen los servicios que se ofrecen a los desarrolladores. Cada servicio tiene una tarea muy específica y aborda las inquietudes discutidas enSeccion 3. Ahora explicamos con más detalle cómo funcionarán estos servicios.

*Definición de contexto.*Este servicio implementará los diferentes contextos que se presentan en cada escenario. Para el caso que estamos considerando, los dos contextos que hemos identificado tienen varios elementos en común. Así, el servicio de definición de contexto servirá como una especie de base de datos para todos los contextos y reutilizará información sobre sus componentes, como en algunos casos (como ocurre en nuestro caso conC_0yC_1), hay elementos comunes.

Como parte de la definición del contexto, se deben modelar los dispositivos potenciales y sus capacidades, se deben proporcionar identificadores únicos a los contextos y se deben proporcionar estrategias para detectar y reaccionar ante las transiciones entre contextos. Como parte del servicio, se deben incluir varias primitivas, como una función que pueda determinar todas las cosas que forman parte de un contexto determinado, en un momento determinado. El servicio también debe realizar un seguimiento de los diferentes contextos que existen durante la vida útil del sistema (hasta una cantidad limitada de memoria de respaldo).

En nuestro caso, los desarrolladores deberían modelar una gran cantidad de dispositivos, incluidos teléfonos inteligentes, gafas inteligentes y los circuitos a bordo del automóvil. Los desarrolladores también deben modelar las cosas humanas que forman parte de los contextos, como Anne y Bob (es decir, operadores en el sentido general). El servicio debería permitir a los promotores expresar las relaciones de propiedad (por ejemplo, Ana tiene un coche),

relaciones de intercambio de información (por ejemplo, el automóvil de Anne comparte información sobre Anne) e información de propósito (por ejemplo, el automóvil de Anne comparte información sobre Anne para cumplir la meta)*fix la tubería*). Con toda esta información se pueden deducir contextos y cambios de contextos de forma automática sin necesidad de actualizaciones manuales. Siempre que se detecta un nuevo contexto, se genera un nuevo identificador único para este nuevo contexto y se crea una relación padre-hijo para representar la transición entre contextos.

*Implementación de Modelos de Confianza.*El caso de uso que estamos analizando tiene diferentes modelos de confianza o reputación que es necesario implementar. Este servicio permite la identificación e implementación de los diferentes componentes que constituyen un modelo de confianza o reputación, según la metodología descrita en[18,21].

El servicio define las entidades fiduciarias y sus relaciones de confianza, que en nuestro caso significa Anne, Bob, el DS y todo lo que entra en escena. Asimismo, el servicio define qué entidades pueden calificar a qué otras entidades. En este caso, puede haber sensores y supervisores que puedan actuar como fuentes de reputación sobre Alice y Bob (es decir, operadores).

El servicio también apoya la creación de motores de confianza y reputación. Por lo tanto, los desarrolladores pueden especificar qué factores (es decir, entradas) acepta el motor, cómo se pueden actualizar estos factores y cómo se combinan para generar una puntuación de confianza o reputación.

En cuanto a nuestro caso de estudio, hemos visto que cada cosa puede mantener una relación de confianza con el sistema de despacho. Los desarrolladores podrían implementar diferentes modelos según las capacidades de las cosas o la información disponible para ellas. Como ejemplo, consideremos la relación de confianza entre el DS y la PDA corporativa de Anne. El primer paso para los desarrolladores debería ser modelar el sistema de despacho y la PDA como entidades fiduciarias. Luego, los desarrolladores deberían pensar en cómo el modelo de confianza calcula el valor de confianza de sus relaciones de confianza. En nuestro ejemplo, considere que el equipo de TI de la empresa revisa la PDA cada semana. El equipo de TI proporciona un informe sobre posibles problemas o vulnerabilidades detectadas en la PDA. Este informe se convierte en un factor objetivo que los desarrolladores pueden utilizar como entrada para el motor de confianza del modelo. Por lo tanto, los desarrolladores podrían implementar un modelo de confianza en el que la confianza se calcule promediando todos los campos del informe. Como parte del modelo, los desarrolladores también podrían agregar un cálculo del umbral de confianza. Por lo tanto, el sistema de despacho podría tomar decisiones de confianza dependiendo de si el valor de confianza de la relación de confianza con la PDA está por encima o por debajo del umbral calculado.

*Recomendación de modelos de confianza.*Este servicio se basa en el servicio de implementación de modelos de confianza y proporciona a los desarrolladores plantillas para modelos de confianza conocidos y ya existentes, incluidos los motores de confianza y los factores utilizados por esos motores. Los desarrolladores pueden modificar esta plantilla o completarla con más información, como las instancias específicas que representarán las entidades de confianza y reputación (por ejemplo, Anne, Bob y supervisores).

En nuestro ejemplo, consideramos que los desarrolladores desean aplicar el modelo de Marsh.[15]para los valores de confianza y para calcular los valores de umbral entre el servicio de despacho y el teléfono inteligente de Anne. Por lo tanto, los desarrolladores pueden elegir el modelo desde un menú desplegable, y esta elección genera todos los archivos de configuración, estructuras de datos y clases (en términos orientados a objetos) necesarios para implementar el modelo. En particular, el DS y el teléfono inteligente de Anne se convierten en entidades de confianza, y el motor de confianza acepta como entradas la utilidad de la colaboración, la importancia de la colaboración y la confianza general (confianza basada en el historial de interacciones). La producción es un valor real resultante de multiplicar estos factores. Los desarrolladores deben crear instancias de estos factores, lo que significa que deben relacionarlos con fuentes de información específicas del escenario. Asimismo, la plantilla genera una función para el cálculo del umbral, que toma como entradas el riesgo percibido, la competencia percibida, la importancia de la colaboración y la confianza general.

*Interoperabilidad de modelos de confianza.*De acuerdo con los requisitos de confianza anteriores, la compañía de gas utiliza los diferentes motores de confianza pertenecientes a los diferentes modelos de confianza de las diferentes cosas para procesar la información que proporcionan. Es probable que las salidas de estos motores adopten formas diferentes. Por ejemplo, el modelo de Marsh arroja valores reales en el intervalo [0, 1], pero otros modelos pueden arrojar valores de confianza en diferentes formatos, incluidos números discretos o etiquetas cualitativas como malo o bueno.

La forma en que el DS procesa los valores de confianza obtenidos de los contextos se puede realizar de diferentes maneras. Dependiendo del escenario, el DS podría obtener un valor de confianza global que deriva de alguna manera de todas las cosas en todos los contextos, o podría calcular un valor de confianza para cada uno de los contextos. Si la opción es tener un valor de confianza global para cada contexto, es posible que el DS necesite generar un valor único a partir de diferentes fuentes. Así, por ejemplo, en el caso del contexto 2 de Anne enFig. 3, los resultados de confianza del automóvil están en forma de valores numéricos, mientras que los resultados de confianza de la PDA están en términos de atributos cualitativos como*Bien*. En este caso, si deseamos combinar estos dos resultados diferentes, el servicio de interoperabilidad de los modelos de confianza debería proporcionar una manera de hacerlo, ya sea mapeando valores cualitativos a numéricos o viceversa.

En resumen, este servicio permite a los desarrolladores definir políticas de mapeo para traducir la semántica de un modelo a la semántica de otro. Una forma de lograr esto sería adjuntar metadatos a los modelos, ya sea como parte de anotaciones en el código o como etiquetas XML/JSON en archivos de configuración. Los metadatos de un modelo de confianza incluyen los valores máximos y mínimos posibles del modelo, ya sea que un valor mínimo signifique desconfianza o simplemente falta de información, o si alguna vez se podrá lograr una confianza total. Siempre que hay una nueva colaboración entre el sistema de despacho y una cosa, estos metadatos se envían junto con el resto de la información, por lo que el sistema puede almacenar esta información y utilizarla siempre que necesite traducir de un modelo a otro.

Dinámica y evolución.La especificación de políticas de reconfiguración se refiere a la especificación de las condiciones en las que se debe cambiar el sistema. Por ejemplo, los desarrolladores pueden especificar que si el valor de confianza de la relación de confianza entre el sistema de despacho y el teléfono inteligente de Anne cae por debajo del umbral especificado por el modelo de confianza (por ejemplo, el modelo de Marsh, como se discutió anteriormente), la interfaz de comunicación debe cortarse y el El sistema de despacho debería buscar otras cosas más confiables en el contexto de Anne de las cuales recuperar la información requerida.

6. Conclusión

El auge del paradigma de IoT está trayendo consigo nuevos desafíos en materia de seguridad y confianza. En este documento, analizamos los desafíos inherentes a la confianza que deben superarse en los escenarios de IoT y presentamos un marco para que lo utilicen los desarrolladores para incluir preocupaciones de confianza en los sistemas de IoT. La arquitectura del marco comprende diferentes capas, donde las capas superiores dependen de las inferiores. El marco garantiza que la confianza se incluya en todas las fases del desarrollo de los sistemas de IoT siguiendo un enfoque proactivo, en lugar de un servicio de último momento, que ha sido el estándar para abordar la confianza hasta ahora. Los puntos clave del marco son las consideraciones de la tríada que comprende los requisitos de confianza, identidad y privacidad y la posibilidad de tener en cuenta la dinámica y la evolución.

Hemos descrito un escenario y un caso de uso que muestran una ejemplificación de IoT y cómo se le aplica el marco. Queda para el futuro trabajar en una implementación del marco, que se referirá principalmente a la implementación de todas las capas intermedias y servicios que forman parte del mismo. Hemos proporcionado algunas sugerencias sobre cómo se puede abordar la implementación para cada servicio. Un paso inicial hacia esto es la inclusión de requisitos de privacidad e identidad en los lenguajes de especificación de requisitos existentes definidos para la confianza, como los basados en SI.•.

Agradecimientos

Esta investigación ha sido parcialmente financiada por el Gobierno español.Ministerio de Economíay FEDER a través de los proyectos PRECISE (TIN2014-54427-JIN) y PERSISTIR (TIN2013-41739-R).

Referencias

[1] Sala de redacción de Gartner, (http://www.gartner.com/newsroom/id/2828722).
[2] ¿Son los usuarios de Facebook más conscientes de la privacidad ahora?, 2012.
[3] El informe Gartner, 2013, (http://www.gartner.com/imagesrv/pdf/Gartner_2013_annual_report.pdf).
[4]L. Atzori, A. Iera, G. Morabito, M. Nitti, El Internet social de las cosas (siot): cuando las redes sociales se encuentran con el Internet de las cosas: concepto, arquitectura y caracterización de la red, Comput. Neto. 56 (2012) 3594–3608.
[5]F. Bao, I.-R. Chen, Gestión dinámica de la confianza para aplicaciones de Internet de las cosas, en: Taller internacional sobre Internet de las cosas autoconsciente, ACM, 2012b, págs.
[6]F. Bao, I.-R. Chen, Gestión de confianza para Internet de las cosas y su aplicación a la composición de servicios, en: Simposio internacional IEEE sobre el mundo de las redes inalámbricas, móviles y multimedia (WoWMoM), IEEE, 2012, págs.
[7] G. Blair, N. Bencomo, RB France, Models@ run.time, Computer 42 (10) (2009) 22–27, doi:10.1109/MC.2009.326.
[8]M. Blaze, J. Feigenbaum, J. Lacy, Gestión de confianza descentralizada, en: Actas del Simposio IEEE sobre seguridad y privacidad de 1996, IEEE Computer Society Press, 1996, págs.
[9]D. Chen, G. Chang, D. Sun, J. Li, J. Jia, X. Wang, Trm-iot: un modelo de gestión de confianza basado en una reputación difusa para Internet de las cosas, Comput. Ciencia. inf. Sistema. 8 (4) (2011) 1207–1228.
[10]F. Fouquet, O. Barais, N. Plouzeau, J.-M. Jézéquel, B. Morin, F. Fleurey, Un modelo de componentes dinámicos para sistemas ciberfísicos, 15º Simposio internacional ACM SIGSOFT sobre ingeniería de software basada en componentes, Bertinoro, Italia, 2012.
[11]H. Hanen, J. Bourcier, Gestión del tiempo de ejecución basada en la confiabilidad de arquitecturas orientadas a servicios, PESOS - 4to Taller Internacional sobre Principios de Ingeniería de Sistemas Orientados a Servicios - 2012, Zurich, Suiza, 2012.
[12]P. Herrmann, H. Krumm, Aplicación de políticas de seguridad adaptadas a la confianza en aplicaciones estructuradas de componentes distribuidos, en: Sexto Simposio IEEE sobre Computadoras y Comunicaciones, 2001, págs.
[13]L. Klejnowski, Y. Bernard, J. Hähner, C. Müller-Schloer, Una arquitectura para agentes adaptables a la confianza, en: 2010 Cuarta Conferencia Internacional IEEE sobre Sistemas Autoadaptativos y Autoorganizados (SASO), IEEE, 2010, págs. 178-183.
[14] M. Li, X. Sun, H. Wang, Y. Zhang, J. Zhang, Control de acceso consciente de la privacidad con gestión de confianza en servicios web, World Wide Web 14 (4) (2011) 407–430, doi :10.1007/s11280-011-0114-8.
[15]S. Marsh, Formalizando la confianza como concepto computacional, Ph.D. tesis, Universidad de Stirling, 1994.
[dieciséis]F. Moyano, Marco de ingeniería fiduciaria para servicios de software, Ph.D. Tesis, Universidad de Málaga, 2015.
[17] F. Moyano, C. Fernández-Gago, J. López, Un marco conceptual para modelos de confianza, en: S. Fischer-Hübner, S. Katsikas, G. Quirchmayr (Eds.), 9ª Conferencia Internacional sobre Confianza, Privacidad y seguridad en los negocios digitales (TrustBus 2012), Apuntes de conferencias sobre informática. Springer Verlag, Springer Verlag, Viena, 7449, 2012, págs. 93-104, doi:10.1007/978-3-642-32287-7.
[18] F. Moyano, C. Fernández-Gago, J. López, Construyendo confianza y reputación en: un marco de desarrollo para la implementación de modelos de confianza, en: A. Jøsang, P. Samarati, M. Petrocchi (Eds.), Octavo Taller Internacional sobre Seguridad y Gestión de la Confianza (STM 2012), LNCS. Springer, Springer, Pisa, 7783, 2013, págs. 113-128, doi:10.1007/978-3-642-38004-4.
[19] F. Moyano, C. Fernández-Gago, J. López, Un marco para permitir requisitos de confianza en aplicaciones de nube social, Requisitos Eng. 18 (2013) 321–341, doi:10.1007/s00766-013-0171-x.
[20]F. Moyano, C. Fernández-Gago, J. López, Hacia la ingeniería de futuros sistemas de Internet conscientes de la confianza, en: X. Franch, P. Soffer (Eds.), 3er Taller Internacional sobre Ingeniería de Seguridad de Sistemas de Información (WISSE 2013), LNBIP, Springer-Verlag, Valencia, España, 2013, págs. 490–501.
[21]F. Moyano, C. Fernández-Gago, J. López, Un enfoque basado en modelos para generar confianza y reputación en servicios de software, J. Netw. Computadora. Aplica. 69 (2016) 134-151.
[22]F. Paci, C. Fernandez-Gago, F. Moyano, Detección de amenazas internas: un marco consciente de la confianza, en: IEEE (Ed.), 8ª Conferencia Internacional sobre Disponibilidad, Fiabilidad y Seguridad (ARES), 2013, págs. 121 –130.
[23] H. Psaier, L. Juszczyk, F. Skopik, D. Schall, S. Dustdar, Monitoreo del comportamiento en tiempo de ejecución y autoadaptación en sistemas orientados a servicios, en: 2013 IEEE 7ma Conferencia Internacional sobre Autoadaptación y Autoadaptación Sistemas organizativos (SASO), 0, 2013, págs. 164-173, doi:10.1109/SASO.2010.44.
[24] Y. Qin, QZ Sheng, NJ Falkner, S. Dustdar, H. Wang, AV Vasilakos, Cuando las cosas importan: una encuesta sobre Internet de las cosas centrada en datos, J. Netw. Computadora. Aplica. 64 (2016) 137-153, doi:10.1016/j.jnca.2015.12.016.

[25]YB Saied, A. Olivereau, D. Zeghlache., Diseño de sistemas de gestión de confianza para Internet de las cosas: un enfoque multiservicio y consciente del contexto, Comput. Seguro. 39 (2013) 351–365.
[26]Q. Vu, S. Hassas, F. Armetta, B. Gaudou, R. Canal, Combinando confianza y autoorganización para un mantenimiento sólido de la coherencia de la información en masas perturbadas, en: Quinta Conferencia Internacional IEEE sobre Autoadaptación y Autoorganización Sistemas (SASO), IEEE, 2011, págs. 178–187.
[27]Z. Yan, C. Prehofer, Gestión autónoma de confianza para un sistema de software basado en componentes, Dependable Secure Comput. Traducción IEEE. 8 (6) (2011) 810–823.