D. Ferraris y C. Fernández-Gago y R. Román y J. López, "Una encuesta sobre marcos de modelos de confianza de IoT",*La revista de supercomputación*, 2023.
http://dtohhimi.ohjrohgramourna1a0mira1F0S0tu7pag 27pu0t2en3gramo-05765-4
NIC Lahbt.tpPAG/ s:/bdyoohici.aohtrg 1 ion0s:.10h0t7 tp/ss1:1/2/2w7ww0,2norte3i-0 cs5.7tu6metro5a-4.es/publicaciones

Una encuesta sobre los marcos de los modelos de confianza de IoT

Davide Ferraris[1] · Carmen Fernández-Gago[1] · Rodrigo Román[1] · Javier López[1]

Aceptado: 26 de octubre de 2023

Abstracto

La confianza puede considerarse como un concepto multidisciplinar, fuertemente relacionado con el contexto y que se enmarca en diferentes campos como la Filosofía, la Psicología o la Informática. La confianza es fundamental en toda relación, porque sin ella una entidad no interactuará con otras entidades. Este aspecto es muy importante, especialmente en el Internet de las cosas (IoT), donde muchas entidades producidas por diferentes proveedores y creadas para diferentes propósitos tienen que interactuar entre ellas a través de Internet, a menudo en condiciones de incertidumbre. La confianza puede superar esta incertidumbre, creando una base sólida para facilitar el proceso de interacción entre estas entidades. Creemos que considerar la confianza en el IoT es fundamental, y para implementarla en cualquier entidad de IoT, es fundamental considerarla a lo largo de todo el ciclo de vida del desarrollo del sistema. En este artículo proponemos un análisis de diferentes trabajos que consideran la confianza para el IoT. Nos centraremos especialmente en el análisis de los frameworks que se han desarrollado para incluir la confianza en el IoT. Haremos una clasificación de los mismos aportando una serie de parámetros que creemos fundamentales para considerar adecuadamente la confianza en el IoT. Así, identificaremos aspectos importantes a tener en cuenta a la hora de desarrollar marcos que implementen la confianza en IoT, encontrar brechas y proponer posibles soluciones.

Palabras clave Confianza · Métricas · Modelos · Frameworks · Internet de las cosas (IoT) · Ciclo de vida de desarrollo de sistemas (SDLC)

Carmen Fernández-Gago, Rodrigo Román y Javier López han contribuido igualmente a este trabajo.

* Davide Ferraris
ferraris@uma.es

Carmen Fernández-Gago
mcgago@uma.es

Rodrigo Román
rroman@uma.es

Javier López
javierlopez@uma.es

[1] NICS Lab, Universidad de Málaga, Edificio de Investigación Ada Byron, Arquitecto Francisco Peñalosa, 18, 29071 Málaga, España

1. Introducción

El Internet de las Cosas (IoT) es un paradigma que permite a los humanos y a las entidades inteligentes cooperar entre sí de cualquier forma y en cualquier lugar.1]. Además, los ecosistemas de entidades de IoT crecen cada año y "se espera que haya más de 64 mil millones de dispositivos de IoT en todo el mundo para 2025".[1]Esta predicción afirma que el paradigma de IoT definirá cómo estará conectado el mundo. Por eso surgirán muchas oportunidades, pero también muchos problemas.2]. Una manera de mitigarlos la ofrece la confianza. De hecho, una entidad debería interactuar con otra sólo si se establece confianza entre ellas. Sin embargo, debido a la incertidumbre, la interoperabilidad y la heterogeneidad de la IoT, lograr la confianza sigue siendo un desafío. Además, considerando el hecho de que las comunidades de investigación han abordado estos aspectos por separado, debería ser deseable un enfoque holístico [3].

Sin embargo, la confianza es difícil de definir. Se trata de diferentes aspectos y temas que van desde la Filosofía hasta la Informática [3], y depende en gran medida del contexto. Este es un punto fuerte en común con IoT, donde es posible tener diferentes contextos para diferentes entidades. Por lo tanto, si consideramos la confianza en estos contextos, podemos mejorar la protección de dichas entidades permitiendo que solo las de confianza interactúen con ellas.

Además, la confianza depende en gran medida de otras propiedades como la seguridad y la privacidad [4,5] y estas relaciones son aún más importantes durante el desarrollo de una entidad de IoT [6]. Declaración también reivindicada por Mohammadi et al. [7], donde los autores declaran que los mecanismos de confianza son fundamentales en el desarrollo de entidades de IoT y esta tarea requiere más investigación.

Por estas razones, en nuestra opinión, es crucial considerar la confianza desde las fases iniciales del Ciclo de Vida de Desarrollo del Sistema (SDLC) para desarrollar las relaciones de confianza entre las entidades de manera sistemática. Este enfoque puede ayudar a proteger las entidades y darles reglas de comportamiento importantes durante las interacciones con otras entidades.

Durante la interacción de dos entidades bajo una perspectiva de confianza, podemos afirmar que normalmente hay al menos dos actores involucrados: el fideicomitente y el fiduciario. El fideicomitente es quien confía activamente y el fiduciario es quien mantiene el fideicomiso. El fideicomitente necesita que el fiduciario realice una acción o cumpla un objetivo considerando un contexto particular. Este objetivo no es alcanzable por el fideicomitente por sí solo. En este caso, las métricas de confianza son útiles para calcular un nivel de confianza que ayude al fiduciario a decidir si se puede confiar en un fideicomisario.8]. Por lo tanto, este valor debe calcularse antes de que los dos actores comiencen la colaboración. Además, el nivel de confianza podría cambiar con el tiempo, positiva o negativamente, debido al comportamiento correcto o incorrecto del administrador [9].

En este artículo analizaremos cómo se ha considerado la confianza y el IoT durante los años en el estado del arte y qué marco para desarrollar la confianza en el IoT se ha desarrollado.

Para realizar dicho análisis, nos centraremos en varios parámetros que consideramos importantes para implementar la confianza en IoT. Además, clasificamos los

[1]https://techjury.net/blog/internet-of-things-statistics/.

Los marcos de IoT existentes consideran aspectos importantes como las fases del SDLC (es decir, obtención de requisitos), dominios relacionados con la confianza (es decir, seguridad y privacidad) y actividades generales relacionadas con la confianza (es decir, el proceso de toma de decisiones). En la literatura existen muchas otras encuestas sobre confianza e IoT [10–13], pero hasta donde sabemos, no hay encuestas que analicen la relación entre confianza e IoT durante todo el SDLC. Con este artículo queremos llenar este vacío.

El documento está estructurado de la siguiente manera, en la Sección.2, analizaremos el concepto de confianza y marcos de gestión de confianza, y cómo se han definido en el estado del arte a lo largo de los años. Insecto.3, discutiremos sobre IoT y sus conexiones con la confianza. Luego, en la Sec.4Presentaremos los marcos existentes que implementan la confianza en IoT. Insecto.5, explicamos la metodología utilizada para analizar los marcos y, en el Apartado.6, haremos una clasificación de los frameworks según los parámetros explicados. Finalmente, en la Sección.7, describimos desafíos y cuestiones que permanecen abiertas y en8 Concluimos el artículo y discutimos sobre el trabajo futuro.

2 Confianza y gestión de la confianza

En esta sección, en primer lugar, analizaremos cómo se puede definir la confianza presentando varias definiciones definidas por los autores en el estado del arte. Luego, discutiremos sobre gestión de confianza, métricas de confianza y modelos de confianza.

2.1 Análisis del concepto de confianza

“La confianza es un fenómeno común” [14], pero también es un concepto difícil de definir “porque es un concepto multidimensional, multidisciplinario y multifacético [15]”. El Diccionario Cambridge define la confianza en inglés británico como “creer que alguien es bueno y honesto y no te hará daño, o que algo es seguro y confiable”, en inglés americano como “tener confianza en algo o creer en algo”. alguien” y en inglés de negocios como “creencia de que puedes depender de alguien o algo”.[2]Así, tenemos tres definiciones similares, pero no iguales, en el mismo diccionario sobre la misma palabra en tres ámbitos similares, que pueden dar una idea de la dificultad para definir confianza.

Sin embargo, analizando estas definiciones, existe una distinción respecto de personas (“alguien”) y objetos (“algo”). En el primer caso, hay una referencia al respeto a la bondad y honestidad de la persona en quien confiamos y que no nos hará daño. En este último caso nos referimos al objeto dando a entender que es seguro y confiable y básicamente que su utilización no nos perjudicará y funcionará como esperábamos. Así, podemos afirmar que estas definiciones son generales. Además, pueden dar una pista importante de que la confianza está fuertemente relacionada con el contexto.

En el estado del arte existen multitud de definiciones de confianza aplicables a diferentes aspectos. Erickson [dieciséis] afirmó que “la confianza significa muchas cosas para muchas personas”.

[2] http://dictionary.cambridge.org/dictionary/english/trust.

De acuerdo con esta definición, podemos entender por qué es difícil definir y explicar qué es la confianza. Además, muchos campos de estudios como la Sociología, la Psicología, la Filosofía y las Tecnologías de la Información tienen que abordar la confianza de diferentes maneras. Por esta razón, McKnight [17] afirmó que "la confianza ha sido definida de tantas maneras por tantos investigadores diferentes de todas las disciplinas que se necesita urgentemente una tipología de los distintos tipos de confianza".

Así, dar sentido a la confianza es un desafío que muchos autores han abordado en los últimos años.4,18–24].

Mayer et al. [18] definió la confianza como una "voluntad de ser vulnerable ante otra parte".

McKnight y Chervany [19] explicó que la intención de confianza es "el grado en que una parte está dispuesta a depender de la otra en una situación determinada con un sentimiento de relativa seguridad, aunque sean posibles consecuencias negativas".

Gambeta [20] afirmó que "la confianza (o, simétricamente, la desconfianza) es un nivel particular de probabilidad subjetiva con el que un agente evalúa que otro agente o grupo de agentes realizará una acción particular, tanto antes de que pueda monitorear dicha acción (o independientemente de su capacidad de poder controlarlo alguna vez) y en un contexto en el que afecta a su propia acción".

Mui et al. [21] afirmó que "la confianza es una expectativa subjetiva que un agente tiene sobre el comportamiento futuro de otro en función de la historia de sus encuentros".

Para Ruohomaa et al. [22] "la confianza es el grado en que una parte está dispuesta a participar en una acción determinada con un socio determinado, considerando los riesgos e incentivos involucrados".

Hoffman [4] definió la confianza "como la expectativa de que se proporcionará un servicio o se cumplirá un compromiso".

Jøsang [23] afirmó que "la confianza es un fenómeno personal y subjetivo que se basa en diversos factores o evidencias" y también que "la confianza es la probabilidad subjetiva por la cual un individuo, A, espera que otro individuo, B, realice una determinada acción sobre la cual su el bienestar depende".

Olmedilla et al. [25] especificó que "la confianza de una parte A hacia una parte B para un servicio X es la creencia mensurable de A en que B se comporta de manera confiable durante un período específico dentro de un contexto específico (en relación con el servicio X)".

Finalmente, Agudo et al. [24] definió que la confianza está relacionada con "el nivel de confianza que una entidad que participa en un sistema de red deposita en otra entidad del mismo sistema para realizar una tarea determinada".

Aunque todas las definiciones son diferentes, comparten algún concepto subyacente. Todos los autores citados anteriormente afirmaron que la confianza depende estrictamente de los actores involucrados en una interacción de confianza. Normalmente, hay dos entidades (al menos) involucradas en una interacción de confianza, una es el fideicomitente (la entidad que deposita la confianza) y la otra es el fiduciario (la entidad en la que se deposita la confianza) [5,14,24,26].

Para garantizar una interacción de confianza, podemos afirmar que es necesario que "el fideicomitente confíe en el fiduciario". Analizando esta frase podemos identificar:

1. "el *fideicomitente*" es la entidad que deposita la confianza (confianza activa);
2. "el *fideicomisario*" es la entidad en la que se deposita la confianza (confianza pasiva);
3. "*fideicomisos*" es la acción entre las dos entidades.

La acción de confianza ocurre cuando un individuo (el "fideicomitente") requiere el servicio de otro individuo (el "fiduciario"). Dependiendo del cumplimiento de la acción o de cómo se realice, el nivel de confianza del fideicomitente puede cambiar positiva o negativamente. Esto significa que las interacciones futuras dependerán del resultado de las interacciones pasadas que afectarán el nivel de confianza del fideicomitente.

Un concepto relacionado con la confianza es confiabilidad. Se puede definir como una característica de una persona [5] o de algo [dieciséis] ese es el objeto de la confianza de alguien. En otras palabras, es una característica del fiduciario.

Además, Pavlidis [5] afirmó que "un sistema confiable es un sistema que tiene la capacidad de satisfacer la confianza del cliente y la capacidad de satisfacer sus necesidades declaradas, no declaradas e incluso imprevistas".

McKnight y Chervany [17] definió cuatro conceptos relacionados con la confiabilidad: benevolencia, competencia, integridad y previsibilidad.

- **Benevolencia**: el fideicomitente es importante para el fiduciario y por eso actúa correctamente para no hacerle daño.
- **Competencia**: el fideicomitente es capaz de hacer lo que el fideicomitente quiere (y esta puede ser la razón por la que el fideicomitente pide ayuda al fiduciario).
- **Integridad**: el fiduciario es honesto y actúa de acuerdo a lo que el fideicomitente le pide sin intenciones maliciosas.
- **Previsibilidad**: el fideicomitente puede anticipar el comportamiento del fiduciario y tener conocimiento *a priori* sobre el intercambio.

Según McKnight y Chervany [17], sólo uno de estos cuatro conceptos no es suficiente para establecer una relación de confianza. Por ejemplo, si el fiduciario es honesto pero no tiene competencia para finalizar la acción solicitada por el fideicomitente, entonces este último podría no querer establecer la relación. De hecho, no puede confiar en que el fiduciario realice esa acción. Por otro lado, si el fiduciario es competente pero no es honesto, es probable que no valga la pena establecer la relación porque el fideicomitente no puede confiar en el fiduciario por temor a una posible traición.

La confiabilidad determina si se puede confiar en alguien (o algo); cuanto mayor sea la confiabilidad, mayor será la posibilidad de que se confíe en él. Cuando el nivel deseado de confianza del fideicomitente coincide con la confiabilidad del fiduciario, no hay desequilibrio en la relación de confianza. Las otras posibilidades son confiar menos o confiar más que en la confiabilidad. En el primer caso, hay una pérdida de oportunidades, en el segundo caso hay una pérdida posible porque el fideicomitente es vulnerable.27,28].

La confiabilidad es muy importante tanto para los humanos como para las cosas. Cuando hablamos de algo confiable o de un software, se considera un recurso de alta calidad [29]. Además, un sistema puede definirse como confiable y ser aceptado por los clientes si su capacidad satisface las necesidades de las partes interesadas, no sólo las que ellos preguntan sino también las que no conocen.5].

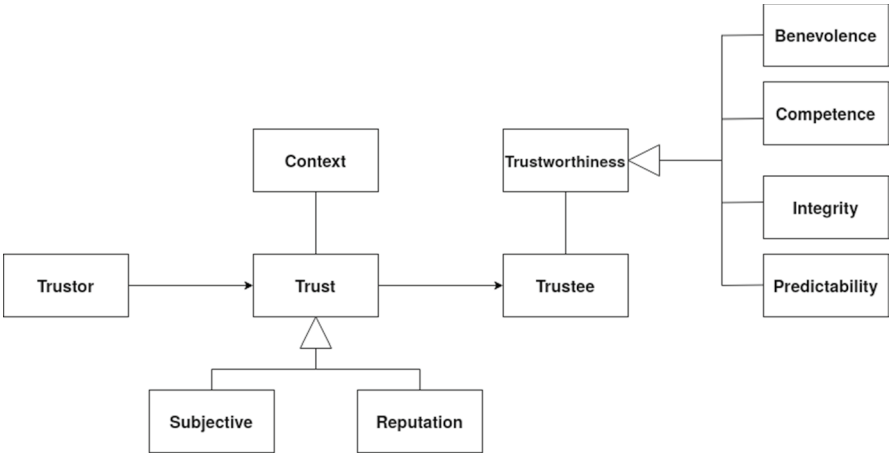

Figura 1 Modelo Conceptual relacionado con la acción de confianza

Fuertemente relacionada con la confianza, la reputación se define como “la opinión que las personas en general tienen sobre alguien o algo, o cuánto respeto o admiración recibe alguien o algo, en base a su comportamiento o carácter pasado”.[3]

Mui [21] afirmó que “la reputación se define como la percepción que una parte crea a través de acciones pasadas sobre sus intenciones y normas”.

Además, la reputación también se define como confianza objetiva.[4]

Podemos decir que la confianza y la reputación están conectadas pero no son lo mismo. Principalmente, la reputación puede ser un parámetro para la decisión de confianza [23].

De hecho, Jøsang [23] afirma que:

“*Confío en ti por tu buena reputación.*"(1)

“*Confío en ti a pesar de tu mala reputación.*" (2)

Éstas son dos definiciones positivas.

Hoffman afirmó que "Se deben definir métricas para medir la confianza y la desconfianza del usuario en un sistema" [4] y Gambetta [20] definió desconfianza respeto simétrico confianza. En aras de la exhaustividad, además de confianza, desconfianza y falta de confianza, Marsh definió también desconfianza y desconfianza [30].

Así, siguiendo estas definiciones, también podemos producir dos afirmaciones negativas:

“*Desconfío de usted a pesar de su buena reputación.*"(3)

“*Desconfío de ti por tu mala reputación.*"(4)

Con estas cuatro definiciones podemos entender mejor que la reputación es un parámetro para considerar la confianza, pero no es el único que afecta el resultado de una empresa.

[3]http://dictionary.cambridge.org/dictionary/english/reputation.
[4]wiki.p2pfoundation.net/Trust_Metrics.

cálculo de confianza. De hecho, por ejemplo es posible confiar en alguien o algo “a pesar de tener mala reputación”.

En la Fig.1, podemos ver un modelo conceptual sobre la confianza. Incluye los actores que realizan una acción de confianza y los parámetros importantes a tener en cuenta.

El modelo conceptual es útil para que los lectores visualicen cómo se puede considerar la confianza para los actores involucrados. Así, podemos ver que el fideicomitente es quien tiene que confiar en el fiduciario. La confianza está conectada al contexto y puede ser subjetiva (es decir, el que confía ya conoce al fiduciario) o puede ser objetiva (es decir, la reputación). Por otro lado, el fideicomisario se elige en función de su confiabilidad, la cual se compone de los cuatro parámetros propuestos por McKnight y Chervany [17].

En la siguiente subsección, analizaremos la gestión de la confianza, las métricas y los modelos.

2.2 Gestión de confianza, métricas y modelos

Para integrar la confianza en cualquier sistema, como los ecosistemas de IoT, se recomienda encarecidamente considerarlo dentro de un marco de gestión de confianza. Sin embargo, un marco suele estar compuesto por tres partes importantes: gestión, métricas y modelos [31]. Es entonces necesario ofrecer una visión general de estos conceptos.

La gestión de la confianza “puede conceptualizarse de dos maneras. En primer lugar, como un proceso según el cual una entidad se vuelve confiable para otras entidades. En segundo lugar, como un proceso que permite evaluar la confiabilidad de otras entidades, que a su vez es explotada para adaptar automáticamente su estrategia y comportamiento a diferentes niveles de cooperación y confianza” [32]. El primer marco de gestión de confianza en la literatura fue PolicyMaker [33]. Blaze lo describió como un sistema de gestión de confianza "que facilitará el desarrollo de funciones de seguridad en una amplia gama de servicios de red". Además, este marco puede considerarse como la forma más general de sistema de gestión de confianza. Más recientemente, Ruan et al. [31] propuso un marco general de gestión de confianza que se compone de tres fases que dependen del contexto:

- **Modelado de confianza**: en esta fase, hay un mapeo de los datos sin procesar de confianza disponibles de los campos en métricas de confianza.
- **Inferencia de confianza**: se centra en propagar y agregar las métricas de confianza obtenidas en toda la red o en la parte de interés.
- **Toma de decisiones**: La toma de decisiones se refiere al uso del conocimiento de confianza producido para respaldar la toma de decisiones. Este proceso permite a la entidad decidir cómo actuar según los datos que ha recopilado y calculado.

De los trabajos citados anteriormente, podemos observar que los modelos de confianza y las métricas de confianza son partes fundamentales de la gestión de la confianza. Además, podemos observar que la confianza está estrictamente relacionada con el contexto y para realizar una decisión de confianza es útil tener una actividad relacionada como la toma de decisiones.

En cuanto a las métricas de confianza, Beth et al. [34] publicó el primer tipo de métrica de confianza moderna. Se compone de un conjunto de reglas utilizadas para derivar la confiabilidad.

valor de un nodo entre 0 y 1, utilizando confianza subjetiva y objetiva. Entonces, Levien [8] definió la métrica de confianza más simple de la siguiente manera. Hay tres elementos:

1. un nodo “semilla” designado que indica la raíz de confianza (S)
2. un nodo "objetivo" (T)
3. un gráfico dirigido

Esto se considera como base para las otras métricas de confianza. Todas las métricas de confianza contienen al menos estos tres elementos. Una métrica de confianza es útil para determinar si el nodo T es digno de confianza o no. Para métricas más complicadas, los bordes pueden contener reglas, pesos o controles. Además, se puede implementar la transitividad y, en este caso, también podemos considerar la propagación y la agregación como métricas de confianza importantes.

Considerando modelos de confianza, Moyano et al. [26] hizo una clasificación de ellos. Este trabajo es importante también porque es útil para extraer algunas características similares de diferentes tipos de modelos. Así, siguiendo esta premisa, es posible crear un marco general que contenga estas características. La clasificación utilizada por Moyano dividió los modelos de fideicomiso en dos categorías principales:

- **Modelos de decisión:**La tarea de estos modelos es hacer que las decisiones de control de acceso sean más adaptables, sustituyendo el proceso de autenticación de dos pasos por una decisión de confianza de un solo paso. Los modelos de políticas y negociación pertenecen a esta categoría. Estos modelos funcionan con políticas y credenciales, otorgando acceso mediante políticas que requieren credenciales específicas.
- **Modelos de evaluación:**Toman en consideración varios parámetros para evaluar la confiabilidad de una entidad. Estos parámetros pueden estar relacionados con modelos de propagación (es decir, los factores de confianza se propagan a lo largo de una cadena de confianza) o modelos de comportamiento (es decir, se miden los factores de confianza). Un subtipo importante de estos últimos son los modelos de reputación, donde las entidades calculan un valor de confianza inicial a partir de la opinión de otras entidades sobre una entidad determinada.

Modelos de políticas (como hacedor de políticas [33]) son un subtipo de modelos de decisión, tienen reglas que se utilizan para dar o no acceso a un recurso. Estas reglas se denominan políticas y se escriben utilizando un lenguaje de políticas [26]. Otro tipo de modelos de decisión son los modelos de negociación (como Trust Builder [35]). Los modelos de negociación de confianza realizan un protocolo de estrategia de negociación, donde dos entidades intercambian credenciales y políticas en un protocolo paso a paso hasta que se toma una decisión de confianza. Esta estrategia se realiza con el fin de proteger la privacidad de las entidades revelando información sensible sólo si es necesaria. Un tipo particular de modelos de evaluación son los modelos de comportamiento. Estos modelos a menudo se construyen de forma sistemática y a través de tres fases [26]:

1. Asignar un valor de confianza a las entidades pertenecientes al sistema.
2. Seguimiento de las entidades y sus atributos.
3. Asigne valores a los atributos monitoreados combinándolos para calcular un resultado final llamado *puntuación de confianza o reputación*.

La puntuación final es un valor que muestra cuánto confía el fideicomitente en el fiduciario y puede ser unidimensional o multidimensional [23]. En el segundo caso, los valores podrían obtenerse de diferentes aspectos de la confianza. Las métricas de confianza se utilizan para calcular estos valores y calculan variables como la seguridad o la utilidad para proporcionar una puntuación total final a las relaciones.26].

Los modelos de reputación son útiles para calcular un valor de confianza inicial, en caso de que el fideicomitente nunca haya tenido interacciones previas con el fiduciario. Estos modelos pueden estar centralizados o distribuidos. En el primer caso, una entidad (un tercero de confianza) recopila información sobre la reputación de las otras entidades y comparte estos valores entre todas las demás entidades. En el segundo caso, cada entidad recopila información sobre otras entidades y la comparte con las otras entidades. En ambos casos, "el modelo podría considerar qué tan cierta o confiable es esta información (por ejemplo, credibilidad de los testigos), y también podría considerar el concepto de tiempo (por ejemplo, qué tan actualizada es la información fiduciaria)" [26]. Los modelos de propagación suponen que algunas relaciones de confianza están disponibles de antemano. Luego, esta información debe ser compartida y difundida a otras entidades. De hecho, estas entidades no tienen conocimiento sobre otras entidades ni si son confiables o no.

3 Gestión de la confianza en el contexto de IoT

Hemos presentado la confianza en general, ahora la describiremos dentro del ecosistema de IoT. Sin embargo, antes de ofrecer una visión general de los marcos de gestión de confianza existentes para IoT, primero debemos presentar qué es IoT. Luego, presentaremos una descripción general de cómo se ha considerado la gestión de la confianza en el ecosistema de IoT.

3.1 Internet de las cosas (IoT)

Una de las primeras tecnologías utilizadas para permitir que las cosas se comunicaran entre sí se llamó Máquina a Máquina (M2M). Como afirmó Watson, M2M "es un término utilizado para describir las tecnologías que permiten a las computadoras, procesadores integrados, sensores inteligentes, actuadores y dispositivos móviles comunicarse entre sí, tomar medidas y tomar decisiones, a menudo sin intervención humana" [36]. En M2M, las "máquinas" utilizan una red para comunicarse con infraestructuras de aplicaciones remotas únicamente con el fin de monitorear o controlar la propia máquina. IoT es una actualización de este paradigma que permite que los objetos interactúen por sí mismos y con el entorno.

Sobre Internet de las Cosas podemos observar que se compone de dos palabras: Internet y cosas. Con estas dos palabras podemos entender el alcance de esta tecnología, que conecta cosas entre sí a través de Internet. Seguramente Internet ofrece muchas posibilidades (es decir, proporcionar comunicación en cualquier parte del mundo), pero también pueden surgir muchos problemas (es decir, amenazas o ataques cibernéticos). La palabra cosa es genérica. Estas cosas pueden ser inanimadas o humanas (es decir, conectadas mediante teléfonos inteligentes, portátiles o tabletas). De hecho, a través del IoT podemos conectar distintos tipos de cosas. Cómo conectarlos de forma protegida y confiable es uno de los principales desafíos en

esta área. En este artículo utilizaremos el término cosas, dispositivos o entidades igualmente para el mismo propósito.

Gazis ha escrito una definición interesante de para qué es útil IoT [37]: “IoT se entiende como la transición (r)evolutiva hacia una era en la que los activos físicos y los activos virtuales serán tratados de manera uniforme y, para todos los efectos, serán en gran medida indistinguibles de los procesos que los involucran. La magnitud del IoT sugiere que unos estándares globales armonizados serán fundamentales para lograr un tratamiento perfecto entre la faceta física y la faceta virtual de las cosas”.

Podemos afirmar que IoT es un concepto y un paradigma que considera la presencia generalizada en el entorno de una variedad de cosas que a través de conexiones inalámbricas/cableadas y esquemas de direccionamiento únicos son capaces de interactuar entre sí cooperando para crear nuevas aplicaciones/servicios y alcanzar objetivos comunes. En este contexto, los desafíos de investigación y desarrollo para crear un mundo inteligente son numerosos y difíciles de implementar. Un mundo donde lo real, lo digital y lo virtual convergen para crear entornos inteligentes que proporcionen energía, transporte y servicios entre las entidades inteligentes. Además, de acuerdo con la heterogeneidad del IoT, podemos afirmar que está compuesto por diferentes entidades desarrolladas por diferentes proveedores, cada uno de ellos con un propósito diferente y un ciclo de vida diferente. Queremos centrarnos en la palabra diferente para dejar claro que se trata de un entorno completamente heterogéneo en todos los aspectos.

Por lo tanto, el objetivo de IoT es permitir que las entidades inteligentes estén conectadas en cualquier momento, en cualquier lugar, con cualquier cosa y con cualquier persona, idealmente utilizando cualquier red de ruta y cualquier servicio.1]. Las cosas pueden volverse reconocibles y volverse “inteligentes” al tomar o permitir decisiones relacionadas con el contexto. Pueden proporcionar información sobre ellos mismos o acceder a información proporcionada por otras cosas. Además, junto con otras entidades inteligentes, pueden ser componentes de servicios complejos. De todos modos, se espera que estas entidades tengan que interactuar entre sí a menudo en condiciones poco claras. Los mecanismos útiles para abordar esta necesidad de información pueden resolverse considerando la confianza como un requisito para superar la incertidumbre. Por lo tanto, con la IoT habilitando hogares y ciudades inteligentes, es posible conectar entidades cotidianas y controlarlas de forma remota. Para facilitar esta implementación, los fabricantes de dispositivos IoT permiten a sus propietarios controlarlos incluso cuando están lejos de su red doméstica. La funcionalidad permite sincronizar los dispositivos conectados y recibir instrucciones de otros dispositivos de entidades inteligentes.[5]y servicios.[6]Un problema está relacionado con el hecho de que los fabricantes de dispositivos inteligentes suelen incluir diferentes tecnologías de comunicación, como Zigbee o Zwave [38]. Estas tecnologías están integradas con protocolos propietarios o uno de los muchos protocolos estándar [37]. Además, normalmente no pueden comunicarse directamente entre sí [39] pero con una estación central que permita las interacciones entre ellos a través de un “intermediario legítimo”. Otro problema está relacionado con el uso de diferentes versiones de la misma tecnología. Por ejemplo, en el caso de Bluetooth Low Energy (BLE), no siempre se garantiza la compatibilidad con versiones anteriores del mismo protocolo [40]. Una solución adoptada para este problema ha sido tradicionalmente que los fabricantes creen su propio centro inteligente de IoT.

[5] http://www2.meethue.com/en-gb/.
[6] https://developer.amazon.com/alexa.

correspondiente a los dispositivos compatibles [41]. Teniendo en cuenta estos aspectos, los desafíos para construir un conjunto de entidades inteligentes heterogéneas que puedan cooperar entre sí se vuelven más difíciles.

Sin embargo, podemos distinguir entre dos arquitecturas principales de IoT: centralizada o distribuida. En un enfoque centralizado, tenemos un dispositivo central llamado centro inteligente, que es una puerta de enlace que generalmente administra un grupo de dispositivos en su mayoría pasivos. El control principal pertenece al propio centro. La principal amenaza relacionada con este tipo de arquitectura es que, cuando el centro inteligente se ve comprometido o deja de funcionar, toda la arquitectura fallará. Como Singh [42] afirmó, se pueden realizar muchos ataques contra el centro del hogar inteligente. Un ataque de modificación de mensajes o un ataque de repetición son posibles ejemplos de ataques que pueden tener un impacto importante en un entorno doméstico inteligente. Por ejemplo, utilizando una señal repetida, el atacante puede enviar indefinidamente un comando para abrir y cerrar continuamente una ventana. Por otro lado, con un ataque de modificación de mensajes, el atacante puede modificar un parámetro establecido por el usuario o por el sistema. Así, en caso de incendio, por ejemplo, se puede modificar el nivel umbral relacionado con la detección de humo y esto puede provocar que la alarma se encienda demasiado tarde o permanezca apagada. Este es un riesgo para la seguridad y puede tener consecuencias graves para todos los que viven en la casa inteligente o para los vecinos. Por otro lado, en un enfoque distribuido, todas las entidades tienen reglas determinadas [43]. Por lo general, cuando se cumple una condición, el dispositivo relacionado ejecutará una acción local e independientemente sin un comando de smart hub. Básicamente, se espera una comunicación entre pares en este tipo de red [44]. Según Román et al. [43], el mayor riesgo en una arquitectura distribuida radica en que las entidades no están bien protegidas como lo está la unidad central en una arquitectura centralizada. De hecho, si un atacante sabe cómo apuntar a un nodo en particular, se verá comprometido, por ejemplo, filtrando información privada. De todos modos, existen posibles diferentes tipos de esta arquitectura, como la propuesta por Parra [45] donde algunos nodos están en medio de la comunicación. Es una especie de mezcla entre una arquitectura centralizada y distribuida donde surge un problema en caso de que uno de estos nodos intermedios falle. Si esto sucede, la arquitectura también quedará parcial o totalmente dañada.

De todos modos, estas arquitecturas se han considerado para crear marcos utilizados en IoT [3,46] y algunas de estas estructuras se pueden aplicar a diferentes campos de IoT, como ciudades inteligentes, redes inteligentes o hogares inteligentes [45]. En cuanto a las redes inteligentes, algunas de estas arquitecturas son bien conocidas en los sistemas de control industrial [47] donde las redes se dividen en dos o más partes, utilizando firewalls para proteger las redes más vulnerables de ataques directos explotados a través de Internet. Este enfoque mejora la seguridad, la confianza y la privacidad [48]. De todos modos, independientemente de la arquitectura, para interactuar, estos objetos tienen que comunicarse entre sí. Como hemos demostrado anteriormente, la comunicación puede resultar difícil entre diferentes proveedores por muchos problemas diferentes. La confianza puede ayudar a abordar esta necesidad y hacer que las entidades confíen entre sí durante su comunicación.

3.2 Confianza en la IoT

En el estado del arte, varios autores han propuesto cómo considerar la confianza en el IoT. Sin embargo, debido a la incertidumbre, la interoperabilidad y la heterogeneidad del entorno de IoT, lograr la confianza sigue siendo un desafío.

Leister et al. [49] afirmó que "el Internet de las cosas conectará muchos dispositivos diferentes. Para lograrlo, los usuarios deben estar dispuestos a confiar en los dispositivos y en la comunicación que se produce automáticamente". Además, debido a que estos aspectos han sido abordados por comunidades de investigación no relacionadas, es deseable un enfoque holístico [3].

Azzedin et al. [50] afirmó que el campo de la confianza relacionado con IoT aún está en su infancia. Con su trabajo quieren "crear la conciencia y la necesidad de modelar la confianza en el comportamiento" en las áreas de fusión de información e IoT. De hecho, la confianza en IoT es muy importante porque para iniciar una interacción, los dispositivos inteligentes deben confiar entre sí.

Elkhodr et al. [51] se centró en el hecho de que en IoT es muy importante conocer el origen de la fuente de datos y comprender si es posible confiar en ellos o no. Además afirmaron que "esto requiere no sólo procesos de recopilación de datos precisos, seguros y correctos; sino también el suministro de la procedencia de los datos durante todo el ciclo de vida de un dispositivo IoT y los datos que produce". Además, en la mayoría de los casos, las entidades inteligentes que interactúan nunca se han comunicado entre ellas en el pasado. Por lo tanto, no se conocen directamente. Por esta razón, es importante crear una relación de confianza que permita que los dispositivos inteligentes se comuniquen entre ellos de manera confiable.52]. Además, ser confiable es un requisito previo para ser aceptado socialmente por un software o una entidad de IoT [27]. De hecho, si no hay confianza, será difícil vender un producto y aumentar su mercado.53].

Wang y cols. [54] afirmó que "indicar confianza o desconfianza en un nodo es una cuestión clave en la gestión de la confianza de IoT".

Yan et al. [52] declaró que "la gestión de la confianza juega un papel importante en la IoT para la fusión y extracción de datos confiables, servicios calificados con conocimiento del contexto y una mayor privacidad del usuario y seguridad de la información. Ayuda a las personas a superar las percepciones de incertidumbre y riesgo y promueve la aceptación y el consumo de servicios y aplicaciones de IoT por parte de los usuarios".

Fernández-Gago et al. [3] afirmó que "el Internet de las Cosas (IoT) es un paradigma basado en la interconexión de objetos cotidianos. Se espera que los elementos involucrados 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 IoT que existan mecanismos que ayuden a superar la falta de certeza. La confianza puede ayudar a lograr este objetivo". Sin embargo, en un entorno como el IoT, la confianza puede estar relacionada con diferentes aspectos. Por tanto, existe la posibilidad de que en un mismo escenario puedan existir diferentes contextos con diferentes relaciones de confianza. De hecho, IoT es dinámico y este aspecto afecta las relaciones de confianza porque si se confía en una cosa en un contexto particular, esto podría no ser cierto en otro contexto. En este caso, si el contexto cambia, la relación de confianza también puede cambiar.

Además, la reputación es muy importante en un entorno de IoT, especialmente si dos o más entidades no tuvieron ninguna interacción pasada entre ellas, la reputación se puede utilizar como parámetro para definir el nivel de confianza inicial. Este es un aspecto general, pero

Es muy importante también para el IoT. Hussain et al. [55] afirmó que la confianza y la reputación siempre son importantes en cualquier tipo de interacción entre entidades de IoT, incluso esta relación es entre humanos a humanos (H2H), máquinas a máquinas (M2M) o interacciones entre humanos y máquinas (HMI). Propusieron "un modelo de evaluación de confianza consciente del contexto para evaluar la confiabilidad de un usuario en un IoT basado en niebla (FIoT)". Consideraron un “sistema de evaluación basado en la reputación y la confianza de múltiples fuentes y consciente del contexto que ayuda a evaluar la confiabilidad de un usuario de manera efectiva”. Ursino et al. [56] afirmó que “si una cosa puede tener un perfil y un comportamiento como un humano, no está fuera de lugar extender el concepto de confianza y reputación a las cosas y definir enfoques ad hoc para su cómputo”. Los autores estudiaron la confianza y la reputación de una "cosa" en múltiples escenarios de IoT y propusieron un enfoque consciente del contexto para evaluarlos. Sin embargo, han modelado de manera diferente la forma en que se consideran las cosas y las personas. De hecho, han observado que “el número y la variedad de cosas disponibles está llevando a los investigadores a modelar la realidad existente como un conjunto de IoT interactuando entre sí, en lugar de un IoT único”. Este es un punto interesante a tener en cuenta durante el desarrollo de una entidad IoT inteligente.

Igualmente a la gestión de confianza,**manejo de reputación**puede ser centralizado o distribuido [43]. En una arquitectura centralizada hay un nodo que contiene todos los valores de reputación de todos los nodos. Por otro lado, en una arquitectura distribuida cada nodo debe almacenar por separado los valores de reputación de todos los demás nodos del sistema. En un sistema de reputación, cuando un dispositivo IoT quiere establecer una conexión con otro dispositivo, necesita un valor de reputación para crear una instancia de su nivel de confianza inicial. En una arquitectura centralizada (es decir, con un centro de IoT central), para obtener el valor de reputación del otro dispositivo de IoT, la entidad de IoT solicitante pregunta al centro central el valor de reputación. Una vez obtenido el valor, el dispositivo IoT solicitante decidirá si procede con el intercambio de información. Por otro lado, en una arquitectura distribuida, cada dispositivo IoT posee cierta información sobre las otras entidades y si está a punto de crearse una nueva conexión, las entidades IoT intercambian su información entre ellas. En ambas arquitecturas, la confianza es crucial para decidir en qué nodo confiar e interactuar o no. En resumen, podemos afirmar que en un enfoque centralizado la cantidad de datos que deben calcular los dispositivos IoT individuales es menor, pero esto crea un cuello de botella en las comunicaciones. Por otro lado, en el enfoque distribuido, los dispositivos IoT necesitan más potencia computacional.

Sin embargo, hay investigadores que investigan cómo es posible reducir la cantidad de datos que se computan en IoT. Li y col. [57] se centró en que IoT permite la conexión entre muchos dispositivos heterogéneos y la confianza es fundamental para evaluar la calidad de los diferentes servicios disponibles. Además, consideran que el contexto es crucial porque es posible confiar en un servicio para un propósito particular y no para otro. Propusieron un “nuevo modelo de confianza consciente del contexto para dispositivos IoT livianos” sin almacenar información sobre los comportamientos pasados de los nodos debido a su poder computacional limitado. De hecho, el modelo sólo necesita una cantidad limitada de información almacenada y puede resistir varios ataques, como hablar mal y encender y apagar.

Otra posibilidad la presentan Fortino et al. [58], donde sugieren “utilizar las capacidades de dispositivos cercanos que tengan recursos adecuados, siempre que pongan a disposición sus recursos de forma gratuita o con un costo determinado”. Proponen una solución

“donde cada dispositivo IoT está asociado a un agente que ayuda a su dispositivo a elegir socios confiables para sus tareas”. Utilizan la reputación como “contramedida contra dispositivos IoT maliciosos”.

En un trabajo posterior, Fortino et al. [59] también han analizado las arquitecturas de IoT actualizadas explicando cómo integrarlas con nodos que pertenecen tanto al paradigma de computación en la niebla como en el de borde. La informática de borde se utiliza mucho en IoT, Sadique et al. [60] investigó una integración de la gestión de confianza distribuida en IoT a través de tecnología informática de punta, considerando la escalabilidad y la heterogeneidad de los dispositivos de IoT. Además, Junejo et al. [61] propuso un “sistema de gestión de confianza para sistemas ciberfísicos habilitados para niebla”. Consideran los valores de confianza calculados por su modelo para evaluar un factor de credibilidad para cada nodo del sistema. Este factor ayuda a evitar y aislar nodos de niebla maliciosos y preservar los demás.

Además, sobre la computación en la niebla y la confianza, Alemneh et al. [62], propuso un sistema de gestión de confianza bidireccional para la computación en la niebla. Los autores pretenden que garantizando confianza también se puede proporcionar seguridad y privacidad. Más específicamente, propusieron un “sistema de gestión de confianza basado en la lógica que permite a un solicitante de servicios verificar si un proveedor de servicios puede brindar servicios confiables y seguros y le permite al proveedor de servicios verificar la confiabilidad del solicitante de servicios”.

En resumen, en el estado del arte la confianza y el IoT han sido investigados por varios autores y algunos de ellos han propuesto diferentes marcos para incluir la confianza en un sistema o software. En la siguiente parte, presentaremos marcos desarrollados para incluir la confianza en IoT y también algunos marcos generales (no específicos para IoT) que se pueden utilizar (aunque con un impacto menor) en IoT.

4 marcos para la confianza y la IoT

En esta sección, presentamos marcos desarrollados en el estado del arte para incluir la confianza en IoT. Hemos elegido estos trabajos porque cada uno de ellos presentó enfoques interesantes para calcular la confianza de diferentes maneras y utilizando varias arquitecturas. Incluso si algunos de ellos no son recientes, hasta donde sabemos, las ideas que presentan siguen siendo valiosas. Sin embargo, cada uno de los trabajos que aquí presentaremos tiene fallas. Los discutiremos en la Sección.6, donde comparamos todos los marcos proporcionados en esta sección de acuerdo con seis parámetros importantes.

Sin embargo, hemos destacado cómo IoT es un entorno dinámico y heterogéneo, por este motivo determinar la intención real de los dispositivos es un dilema fundamental para un ser humano. Por lo tanto, para ayudar a los dispositivos a unirse a una red IoT de manera correcta, Køien [63] propuso un sistema lógico subjetivo para modelar la interacción de confianza entre humanos y dispositivos. Por lo tanto, el autor estudió la confianza en un dispositivo y servicios de IoT en enfoques multifacéticos de software/hardware considerando propiedades de confianza como la transitividad, la integridad o la benevolencia.

En IoT, también podemos considerar la Nube de Cosas (CoT). Abualese et al. [64] afirmó que CoT es un paradigma fuertemente utilizado por el gobierno electrónico y, en este aspecto, la confianza es de importancia crítica y también un desafío. Así, propusieron un marco para mejorar la confianza entre los dispositivos IoT conectados a la nube. Su estructura se compone de cuatro capas. Uno de ellos está dedicado a la confianza para autenticar la

Dispositivos de IoT. Utilizaron varios métodos de autenticación “para diferenciar el control de acceso de cada dispositivo”. Para abordar la baja potencia de los nodos de IoT, Fortino et al. [sesenta y cinco] definió un CoT que virtualiza dispositivos físicos en el entorno de la nube y los integra con agentes de software para cumplir con sus responsabilidades. Teniendo en cuenta los parámetros y un número adecuado de participantes, demostraron que su algoritmo CoT Agent Grouping (CoTAG) convergía rápidamente para tratar con agentes no confiables y gastos de cálculo. CoTAG considera la confianza mutua, como la reputación local y la votación adecuada.

Considerando la red de sensores inalámbricos (WSN), Ali et al. [66] describió un esquema de confianza para WSN, donde se ha considerado la agregación de datos para componentes móviles externos para distribuir los datos hacia la estación base. Dichos componentes eran sensores portátiles o móviles inteligentes que representaban grupos en redes de IoT. Los autores emplearon un algoritmo de enrutamiento basado en clústeres de distribución beta y un factor de olvido dinámico para reducir la manipulación de la confianza por parte de componentes maliciosos.

Mendoza et al. [67] propuso un marco de gestión de confianza distribuida de IoT que considera la interacción directa, como el descubrimiento de vecinos y la observación indirecta (es decir, intercambio de tablas de confianza, recomendación de evaluación y puntuación de actualización). Los mecanismos de cálculo de la confianza local se dividieron en diferentes fases iniciadas por la asignación de valores negativos/positivos a nodos honestos/deshonestos.

Pal et al. [68] propuso un marco de gestión de confianza centrado en mecanismos de control de acceso (es decir, modelos de decisión) que mejoran los procesos de toma de decisiones en condiciones de incertidumbre. Proporcionaron una gestión de identidad basada en atributos. En su modelo de confianza propuesto, la decisión de control de acceso se ha tomado considerando tres tipos diferentes de confianza: directa, recomendada y derivada. Luego, Bernabé et al. [69] propuso un mecanismo de control de acceso basado en la confianza (TACIoT). Para tomar decisiones autorizadas, este enfoque considera cuatro parámetros: calidad de servicio, reputación, seguridad y relaciones sociales. Por lo tanto, para manejar la incertidumbre de la información, se utiliza un método de lógica difusa, que se basa en evidencia histórica de confianza. Sin embargo, debido a la escasez de evaluaciones sobre la precisión de la confianza, también planearon experimentos sobre características de identidad para garantizar una interacción segura y datos compartidos dentro de las comunidades de manera confiable. Además, Mahalle et al. [70] propuso un modelo de toma de decisiones difuso basado en la confianza para el control de acceso (FTBAC). Para calcular un valor de confianza, el marco considera parámetros como la experiencia, el conocimiento y la recomendación. Están diseñados para obtener privilegios de acceso en una red LoT. Los autores demostraron la flexibilidad y escalabilidad de su trabajo. De hecho, la cantidad de dispositivos no deteriora su eficiencia.

Por otro lado, considerando modelos de evaluación y analizando el hecho de que las tecnologías móviles son habilitadoras de IoT, Bica et al. [71] propuso un marco de seguridad con una arquitectura multicapa que aborda la evaluación de la confianza de las entidades de detección basándose en puntuaciones de reputación calculadas mediante un algoritmo de Bayes. Además, DeMeo et al. [72] propuso un marco de reputación para IoT integrado con un agente de reputación (RA) que actúa dentro de una entidad. Esta RA se separa de la entidad a la que pertenece para estimar un valor de reputación “honesto”. Este es un enfoque interesante, pero es vulnerable a ataques de autopromoción en el caso de que se manipule el dispositivo. Seguramente, una puntuación de reputación otorgada por otra entidad de confianza es más fiable. Además, afirman que sería inviable aplicar efectivamente una

El enfoque basado únicamente en la autenticación aborda cuestiones de confianza en un entorno amplio como el IoT.

Ruan et al. [73] propuso un marco de gestión de confianza para IoT que se basa en la teoría de la medición [74]. Sin embargo, los autores consideraron sólo dos métricas: confiabilidad y confianza. Un aspecto interesante es que han modelado las interacciones entre las entidades de IoT dividiéndolas en cuatro tipos de interacciones: humano/humano, cosas/cosas y humano/cosas (en ambas direcciones). Además, han considerado la reputación para calcular un nivel de confianza que muestre cómo la confianza puede ser útil para reconocer qué nodos son maliciosos o confiables. Sin embargo, solo han analizado dos tipos de atacantes, por lo que su marco sólo es útil contra ciertos tipos de amenazas. Además, Ruan et al. [31] propuso un marco general de gestión de confianza. Está compuesto por tres fases. El primero se llama "Modelado de confianza", en esta fase los datos sin procesar de confianza disponibles se recopilan de los campos y se calculan con métricas de confianza. La segunda fase, denominada "Inferencia de confianza", se centra en propagar y agregar los valores de confianza obtenidos en el sistema. La fase final, "Toma de decisiones", utilizará los valores de confianza calculados en las fases anteriores para respaldar el proceso de toma de decisiones. Cada una de estas fases depende del contexto. Este es un punto de enfoque a tener en cuenta. Sin embargo, este marco no se desarrolló específicamente para IoT y cubre solo una fase del SDLC (la fase de modelado). Entonces, Sharma et al. [75], han presentado un marco genérico para gestionar la confianza en IoT considerando parámetros tanto cualitativos como cuantitativos. Han propuesto una solución de gestión de fideicomisos considerando todos los requisitos útiles para realizar la gestión de fideicomisos. Este marco es interesante, pero su principal debilidad es que solo hay una retroalimentación de la última fase que regresa a la primera. Esta es una gran limitación en caso de que se encuentre algún problema en el medio del marco. Además, otra desventaja es que nunca se ha tenido en cuenta el contexto. Además, Bahutair et al. [76] consideró un modelo de confianza adaptable para los servicios de IoT. La confiabilidad de estos sistemas se evalúa según la utilización de los usuarios. Para determinar si se puede confiar en un sistema o no, un algoritmo procesa varios factores de confianza a través de cuatro etapas diferentes. La primera etapa predice los factores de confianza. La segunda etapa calcula estos parámetros para predecir la confiabilidad del sistema. Luego, en la tercera etapa, se construye un “modelo de uso por factor” para detectar qué tan importante es cada factor en diferentes escenarios. Finalmente, la última etapa se compone de dos modelos. Su objetivo es calcular un valor de confianza según el escenario elegido en la fase anterior.

Recientemente, Battah et al. [77] propuso un marco de confianza general para regular las interacciones de servicios de IoT utilizando sistemas de reputación y tecnología blockchain. Propusieron un esquema de recompensa y penalización a través de una arquitectura personalizable para dispositivos IoT. Para garantizar esto, implementaron contratos inteligentes para almacenar información sin utilizar modelos centralizados.

Según SDLC, solo hay unos pocos trabajos que lo consideran para confianza e IoT. Uno de ellos ha sido presentado por Fernández-Gago et al. [3]. Avanzaron con respecto a los trabajos anteriores introduciendo un marco para ayudar a los diseñadores y desarrolladores a considerar la confianza en IoT. Afirmaron que se deben tener en cuenta los requisitos de privacidad e identidad durante la gestión de la confianza y la reputación para mejorar la confianza. Sin embargo, en este marco hay

no hay retroalimentación entre fases y no hay conexión entre los requisitos de privacidad, confianza e identidad. Finalmente, modelan solo las primeras fases del SDLC. A partir de este trabajo, Ferraris et al. desarrolló un marco de confianza por diseño para IoT [6]. Los autores propusieron un marco para garantizar la confianza durante el desarrollo de una entidad de IoT considerando todo el SDLC. Además, este marco garantiza una planificación cuidadosa desde la perspectiva del desarrollador. Además, partiendo de que la confianza está fuertemente relacionada con otras propiedades como la privacidad y la seguridad, se consideran las posibilidades de conectarlas desde la fase de requerimientos. Otros dos aspectos importantes son la trazabilidad y el contexto. El primero se proporciona entre los diferentes requisitos y entre las diferentes fases del marco. Esto último es fundamental para considerar la confianza en una interacción particular de IoT.

La privacidad en IoT también ha sido considerada por Dwarakanath et al. [78]. Los autores propusieron un enfoque basado en la confianza para el procesamiento distribuido de eventos complejos (TrustCEP). Los autores aprovecharon la confianza entre diferentes usuarios según sus interacciones pasadas. Sin embargo, este modelo de gestión de confianza es eficaz en el caso de que los adversarios sean una minoría del total de nodos.

Otros trabajos centrados en el contexto son los siguientes. Wang y cols. [79] desarrolló un modelo de gestión de confianza contextual (CATrust). Puede usarse tanto para P2P como para IoT y analiza el patrón de comportamiento si el contexto cambia, en lugar de estimar la veracidad considerando datos históricos satisfactorios/insatisfactorios. Al tener en cuenta los mecanismos de filtrado de recomendaciones y poner en cuarentena los nodos deshonestos, CATrust reconoce los nodos en colusión. Luego, Saied et al. [80] diseñó un sistema de gestión de confianza multiservicio y consciente del contexto para IoT para mitigar la falta debido a la heterogeneidad de las entidades. Su modelo proporcionó a los nodos de IoT un valor de confianza dinámico basado en comportamientos pasados para lograr una tarea requerida en el servicio cooperativo y luego convenció a los socios más adecuados para la cooperación. Los autores afirmaron que el sistema propuesto desvinculó las intrusiones de nodos maliciosos. Además, Neisse et al. [81] presentó un marco de confianza dinámico y consciente del contexto para IoT. También han considerado la privacidad y la seguridad, junto con los requisitos de identidad. Se centraron en el hecho de que existe un equilibrio entre privacidad y seguridad y que debe ser abordado no sólo por los investigadores, sino también por la sociedad en general. Sin embargo, reconocieron que una limitación de su enfoque radica en el hecho de que la percepción del contexto puede ser ambigua según los datos recopilados por los sensores utilizados. Por lo tanto, confirman que la consideración del contexto es crucial como requisito previo para un marco eficaz para la IoT.

Finalmente, consideramos marcos relacionados con la confianza en el creciente segmento de Internet social de las cosas (SIoT), Lin y Dong [82] desarrolló un modelo de confianza dinámica SIoT compuesto por factores fundamentales como fideicomitente y fiduciario, contexto, estimación confiable y sus consecuencias). Las características únicas de la confianza SIoT se consideran protección mutua del fideicomitente y del fiduciario. Infiere confianza al explorar características históricas. Actualizar la confianza con resultados de delegación de factores tanto positivos como negativos, y ajustarla considerando la influencia de entornos dinámicos. Además, Magdich et al. [83] propuso un trabajo sobre un estudio sobre la efectividad de la gestión de la confianza en relación con los ataques sociales. Propusieron un modelo de confianza que clasifica los comportamientos de los nodos utilizando máquinas.

Algoritmos de aprendizaje. A través de este aspecto, quieren limitar las posibles interacciones tanto con nodos atacantes como con nodos proveedores de servicios deficientes.

5 Metodología

En este apartado presentaremos los seis parámetros que creemos son fundamentales para considerar adecuadamente la confianza en IoT. Estos parámetros se utilizarán luego para analizar los marcos existentes.

El primero de los seis parámetros está relacionado con los modelos de confianza que se utilizan en los marcos. Los modelos se pueden relacionar con los principales considerados en [26] o pueden estar relacionados con modelos de confianza adaptativa similares al presentado en [41]. Los hemos descrito profundamente en la Sección.2.2.

Luego, consideraremos atributos de confianza como las características de confianza que hemos identificado en el estado del arte. Los presentaremos en la siguiente subsección.

En tercer lugar, tendremos en cuenta qué arquitectura de IoT se ha considerado en el artículo seleccionado. Las arquitecturas más conocidas suelen estar centralizadas y distribuidas como se analiza en [1]. Los hemos descrito anteriormente en la Sección.3.1y creemos que SDLC puede ser útil para planificar cuidadosamente soluciones para la confianza en IoT.

Por lo tanto, creemos que es de suma importancia analizar el SDLC y cómo se le aplican los marcos existentes, y en qué fases se considera la confianza. Podría ayudar a adaptar el desarrollo de la entidad a los múltiples aspectos de la confianza. De hecho, si consideramos la confianza desde el principio del SDLC, podemos comenzar a crear requisitos de acuerdo con ella [84] y dichos requisitos pueden ser útiles en las siguientes fases, como la fase de modelo, donde los requisitos se pueden utilizar para crear diagramas y modelos que predicen cómo la entidad de IoT se comportará e interactuará con otras entidades de IoT bajo una perspectiva de confianza. Estas fases previas serán fundamentales para desarrollar [85], verificar y validar [86] la entidad de IoT. Finalmente, la comunidad investigadora reconoce que al considerar propiedades como la seguridad o la confianza en una fase más temprana del SDLC, podemos evitar problemas más adelante en las fases finales. Este proceso se llama desplazamiento a la izquierda [87,88].

Por lo tanto, consideramos también que se puede mejorar la confianza si se consideran otras propiedades como la seguridad o la privacidad. Los llamamos dominio como lo hemos hecho al desarrollar la metodología TrUStAPIS en [84]. Los presentaremos en las siguientes subsecciones.

Finalmente, consideraremos diferentes actividades relacionadas con la confianza que pueden mejorarla en IoT. Están relacionados con la consideración del contexto, la trazabilidad, la toma de decisiones, el análisis de riesgos y amenazas.

En las siguientes subsecciones, analizaremos los parámetros antes mencionados que no se describieron anteriormente: características del fideicomiso, propiedades conectadas al fideicomiso y actividades relacionadas con el fideicomiso.

tabla 1 Características de la confianza

Directo	[34]
Indirecto	[89]
Transitivo	[15,90]
Dirigido	[15]
Dinámica	[5,9,91]
Dependiente del contexto	[26,89]
Local	[89,90]
Global	[89]
Específico	[92,93]
General	[92,93]
Asimétrico	[94]
Subjetivo	[9,15]
Objetivo	[89]
propiedad compuesta	[9,15]
Mensurable	[15]

5.1 Características de la confianza

Para considerar adecuadamente la confianza en un sistema como IoT, es importante obtener características de confianza. De hecho, según ellos, es posible modelar diferentes aspectos del IoT.

Hemos identificado quince características de confianza que deben tenerse en cuenta para implementar la confianza en un sistema como IoT. Los hemos resumido en la tabla1 donde la primera columna trata sobre la característica y la segunda contiene las obras que definen dicha característica.

A continuación se presentan y describen las características de la confianza:

1. **Directo.**Esta propiedad significa que la confianza se basa en experiencias directas entre el fideicomitente y el fiduciario [34]. En este caso, también podemos decir que la confianza depende de la historia.
2. **Indirecto.**Podemos hablar de confianza indirecta, cuando el fideicomitente y el fiduciario no tuvieron interacciones pasadas. En este caso, la confianza se construye a partir de la opinión y recomendación de otras entidades de confianza del fideicomitente [89].
3. **Transitivo.**También podemos referirnos a la posibilidad de que la confianza sea transitiva [90]. De hecho, la confianza es transferible condicionalmente, como afirmó Yan, podemos imaginar la posibilidad de transmitir/recibir información de confianza a lo largo de una cadena de recomendaciones [15]. Sin embargo, en este caso el contexto es fundamental.
4. **Dirigido.**La confianza también es dirigida porque existe una relación orientada entre el fideicomitente y el fiduciario.15]. Esto significa que si A confía en B, no podemos implicar también que B confíe en A.
5. **Dinámica.**La confianza puede cambiar con el tiempo, pero no depende estrictamente del tiempo. Chang [91] afirmó que “la confianza se construye con el tiempo”. De hecho, un fideicomitente podría confiar en el fiduciario sobre algo en un período de tiempo, pero este nivel de confianza podría cambiar en un período siguiente porque algo podría haber sucedido.5] con el fin de

modificar el nivel de confianza original. Además, como afirmó Grandison [9], la confianza debe poder adaptarse al contexto en el que se ha tomado una decisión de confianza y puede cambiar según diferentes contextos.

6. **Dependiente del contexto.** Como mencionamos antes, la confianza puede cambiar dependiendo del propósito donde se utilice. “En general, la confianza es una creencia subjetiva sobre una entidad en un contexto particular [15].” y más específicamente “donde la confianza de un nodo i en un nodo j varía de un contexto a otro [89]”.
7. **Local.** La confianza puede ser **local** [89] porque depende de la pareja considerada de fideicomitente y fiduciario (es decir, Alice y Bob) y si consideramos otras dos parejas (es decir, Alice y Charlie, y Bob y Charlie), es posible que Alice desconfíe de Charlie, incluso si Bob confía en Charlie. [90].
8. **Global.** Como afirmó Abdelghani, “la confianza, también llamada reputación, significa que cada nodo tiene un valor de confianza único en la red que puede ser conocido por todos los demás nodos [89]”.
9. **Específico.** Podemos afirmar que la confianza puede ser específica [92,93]. Esto sucede porque es posible que el fideicomitente confíe en el fiduciario sólo para una acción o servicio específico.
10. **General.** Por otro lado, la confianza puede ser general [92,93]. La confianza es general si el fideicomitente confía en el fiduciario en general y no sólo para una acción específica.
11. **Asimétrico**. Esto significa que dos entidades unidas por una relación pueden confiar entre sí de diferentes maneras, por lo que el hecho de que A confíe en B no implica que B deba confiar en A.94]. Esto está relacionado con la definición de "dirigido".
12. **Subjetivo.** La confianza es subjetiva porque está relacionada con una opinión personal basada en varios factores (es decir, experiencias pasadas) y estos factores pueden tener diferentes pesos.9]. La confianza es diferente para cada individuo en una situación particular [15].
13. **Objetivo.** Por otro lado, la confianza también puede ser **objetivo** “como cuando la confianza se calcula en función de las propiedades de calidad de servicio (QoS) de un dispositivo [89]”. Además, un parámetro objetivo para calcular la confianza también se conoce como **reputación**.
14. **Propiedad compuesta.** La confianza suele ser una propiedad compuesta porque puede estar compuesta de muchos atributos diferentes. Por ejemplo, como Grandison [9] afirmó que puede estar compuesto por “confiabilidad, confiabilidad, honestidad, veracidad, seguridad, competencia y puntualidad”. Por tanto, la composicionalidad es una característica importante para los cálculos de confianza [15] y cada atributo podría tener un peso diferente.
15. **Mensurable.** Finalmente, la confianza es mensurable. De hecho, “los valores de confianza pueden usarse para representar los diferentes grados de confianza que una entidad puede tener en otra. [15].” Esta característica es la base para el cálculo de un valor fiduciario final durante la gestión del fideicomiso.

Las características antes mencionadas y sus relaciones se explican en la Fig.2.

El círculo exterior significa que las características escritas allí siempre están presentes. Entonces las características dentro del círculo interno siguen siendo importantes en todos los aspectos (es decir, dirigidas y asimétricas). *Transitivo* está escrito en cursiva porque no siempre es cierto y se rellena en un rectángulo separado. Finalmente, podemos ver que hay tres parejas conectadas por líneas de puntos. Estas parejas son mutuamente excluyentes. De hecho, la confianza puede ser específica o general, subjetiva u objetiva y local o global. Al mismo tiempo, la confianza puede ser, por ejemplo, específica, objetiva y global. Finalmente, en el

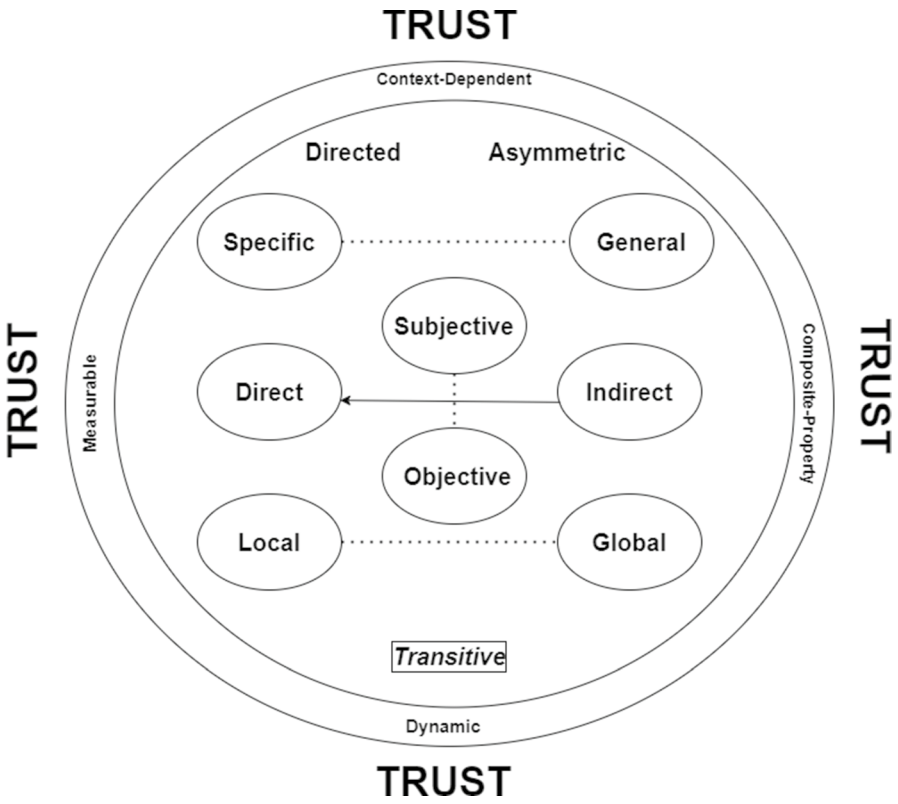

Figura 2 Características de la confianza y sus relaciones.

En el centro del diagrama está la pareja final: directa e indirecta. En este caso, tenemos una flecha que va de indirecta a directa y significa que a veces es posible que la confianza indirecta pueda crear la confianza directa. Esta situación ocurre cuando no hay conocimiento directo (es decir, no hay interacciones pasadas), por lo tanto, para comenzar a construir un valor de confianza, necesitamos un parámetro indirecto y esta interacción está representada por la flecha.

5.2 Propiedades conectadas de confianza

En esta subsección, nos centramos en propiedades relacionadas con la confianza, como la seguridad y la privacidad, a las que también nos referiremos como dominios. En el estado del arte, varios autores resaltaron la importancia de considerar la confianza junto con otras propiedades.

Según Hoffman et al. [4] y Pavlidis [5] la confianza depende en gran medida de otras propiedades o dominios (es decir, privacidad, identidad y seguridad). Además, en el estado del arte existen varios trabajos sobre propiedades fiduciarias que proponen una clasificación de las mismas [15,95]. Algunas de estas propiedades han sido consideradas por

múltiples autores en los años siguientes. Sin embargo, nos centraremos en los presentados por Hoffman y Pavlidis que básicamente contienen también a los demás.

Hoffman [4] propuso un modelo de confianza que considera las siguientes propiedades relacionadas con la confianza: confiabilidad y disponibilidad, privacidad, mecanismos de auditoría y verificación, seguridad, usabilidad y expectativas del usuario.

Pavlidis también considera la confiabilidad, la privacidad, la seguridad y la usabilidad [5]. El autor considera también la disponibilidad como una subpropiedad de la seguridad. Además, tiene en cuenta la seguridad y la mantenibilidad.

Nos centramos en las propiedades tomadas en consideración por ambos autores. Son los siguientes:

- **Disponibilidad.**Significa que las acciones de los sistemas no se pausan ni se detienen por largos periodos.
- **Privacidad**. La privacidad se refiere a algunas características como otorgar confidencialidad o anonimato. Esta propiedad puede entrar en conflicto con la rendición de cuentas [96]. Además, la privacidad también es importante, porque hoy en día los sistemas de información pueden recopilar muy fácilmente una gran cantidad de información personal, este aspecto plantea el riesgo de que esos datos puedan ser divulgados accidental o intencionalmente. Esta situación puede afectar negativamente la confianza de los usuarios. Para Pavlidis, la privacidad tiene cuatro subpropiedades: anonimato, inobservabilidad, seudonimidad y desvinculación. El anonimato es la capacidad de no ser identificado, la inobservabilidad está relacionada con la posibilidad de no ser observado y la seudonimidad da la posibilidad de utilizar alias. La desvinculación puede derivarse del anonimato y la inobservabilidad.
- **Seguridad.**La seguridad se compone de subpropiedades como garantizar que las entidades involucradas en un proceso estén autenticadas, que tengan derechos para acceder a los datos y que los datos no estén dañados. Sin embargo, no es sólo una propiedad de la confianza, como afirmó Yan: “la confianza va más allá de la seguridad. Es una solución para mayor seguridad [15]”. De hecho, para Pavlidis,*seguridad*Debe tenerse en cuenta especialmente en el caso de que no consideremos la confianza en el diseño de un sistema. En este caso, debemos hacer que el sistema sea lo más seguro posible porque es la única defensa contra entidades maliciosas. Por otro lado, si consideramos la confianza, es posible relajar algunas características de seguridad porque se confiará en los usuarios para realizar actividades particulares. Para Pavlidis, la seguridad tiene cinco subpropiedades. La confidencialidad, la integridad y la disponibilidad se conocen como la tríada de la CIA. La autenticación y la autorización son propiedades muy importantes también para la confianza.
- **Usabilidad**. Esta propiedad es importante porque, según Hoffman, si un sistema es difícil de utilizar y comprender, la confianza del usuario podría verse afectada. Además, si un sistema es difícil de utilizar de forma correcta, es posible que se utilice incorrectamente. Esto puede generar problemas y, como consecuencia, puede reducir el nivel de confianza general en el propio sistema [95].
- **Fiabilidad**. Es un atributo que es muy importante para la confiabilidad de un sistema. De hecho, la confiabilidad se ha definido como “la probabilidad de que un sistema realice una función específica dentro de límites prescritos, bajo condiciones ambientales dadas, durante un tiempo específico” [97]. De todos modos, lo consideraremos como un subconjunto de confianza.

- **Seguridad**. La seguridad está fuertemente relacionada con el dominio físico. Evitar que un usuario sufra daños aumentará la confiabilidad del sistema, porque el usuario percibirá el sistema como seguro y confiable.

Por tanto, podemos afirmar que la confianza puede estar conectada a otros dominios o propiedades (es decir, privacidad o seguridad) y estos dominios tienen características fundamentales para definirlos. Este aspecto se tendrá en cuenta para la gestión de fideicomisos. Ferraris et al. [84] tomó en consideración los trabajos de Hoffman y Pavlidis y avanzó especificando seis dominios relacionados con la confianza: seguridad, privacidad, identidad, disponibilidad y usabilidad.

5.3 Actividades

En el estado del arte, muchos autores discuten cómo la confianza puede ser mejorada no sólo por otras propiedades, sino también por otras actividades como la toma de decisiones.98, 99], trazabilidad [100,101], gestión de riesgos [102], análisis de amenazas [103] y consideraciones de contexto [79].

- **Toma de decisiones**: Esta propiedad puede mejorar significativamente la gestión de fideicomisos. Especialmente en un ecosistema como el IoT. De hecho, en este entorno complejo e interconectado, la confianza puede desempeñar un papel fundamental a la hora de guiar las decisiones. Los tomadores de decisiones pueden confiar en datos confiables de IoT para optimizar procesos, predecir resultados y responder de manera efectiva a las condiciones cambiantes. Como hemos comentado anteriormente, la dinámica es crucial para la confianza y la IoT. Además, los sistemas de gestión de confianza pueden evaluar y cuantificar la credibilidad y confiabilidad de las entidades de IoT, asegurando que las decisiones se basen en datos e interacciones que sean confiables y seguras [99]. Ferraris et al. propuso un proceso de toma de decisiones para resolver conflictos entre la obtención de requisitos en IoT [98]. Este proceso se basa en el Proceso de Jerarquía Analítica (AHP) propuesto inicialmente por Saaty [104].
- **Trazabilidad**: La trazabilidad juega un papel importante en la gestión de la confianza en diversos ámbitos [100]. Al proporcionar un registro transparente y auditable de acciones y transacciones, la trazabilidad proporciona responsabilidad e integridad dentro de los sistemas y procesos. Esta transparencia es esencial para generar confianza entre las partes interesadas. En IoT, la trazabilidad mejora la confianza al proporcionar transparencia, responsabilidad y verificación de datos, acciones e interacciones. Es un componente vital para garantizar que los sistemas de IoT funcionen de manera confiable y segura y al mismo tiempo cumplan con las expectativas regulatorias y de confianza de los usuarios.
- **Gestión de riesgos**: La gestión de riesgos y la gestión de la confianza son conceptos estrechamente entrelazados, particularmente en los campos de la ciberseguridad, los negocios y la toma de decisiones [102]. La gestión de riesgos implica la identificación, evaluación y mitigación de posibles amenazas y vulnerabilidades dentro de un sistema u organización. La gestión de fideicomisos es lo opuesto a lo que describimos en la Sección.2. La conexión entre ambos radica en el hecho de que un sistema sólido de gestión de confianza puede ser decisivo para una gestión eficaz del riesgo. Al evaluar y cuantificar la confiabilidad, las organizaciones pueden tomar decisiones más informadas sobre quién

o en qué confiar, mitigando así los riesgos asociados con entidades que no son de confianza. Una base sólida de confianza y credibilidad es esencial para una gestión eficaz del riesgo, garantizando que los riesgos se gestionen con prudencia y que se mantenga la confianza durante todo el proceso de toma de decisiones.

- **Análisis de amenazas**: El análisis de amenazas es un componente fundamental de la gestión de la confianza en el ámbito de la seguridad cibernética y la evaluación de riesgos [103]. Al identificar sistemáticamente vulnerabilidades potenciales y actores maliciosos, el análisis de amenazas proporciona la información necesaria para implementar medidas de confianza y seguridad. A través de un examen exhaustivo de las amenazas potenciales y su impacto potencial en un sistema, la gestión de confianza puede abordar y mitigar los posibles ataques. Al comprender el panorama de las amenazas, la gestión de confianza puede tomar decisiones informadas sobre los procesos de control de acceso. El análisis de amenazas ayuda a generar confianza al crear un entorno digital más seguro, garantizar la integridad de los datos y aumentar la confianza de los usuarios y partes interesadas. Finalmente, la sinergia entre el análisis de amenazas y la gestión de la confianza es crucial para mantener la seguridad y confiabilidad de los sistemas digitales en un mundo cada vez más interconectado como el llamado IoT.

- **Contexto**: El contexto está en el centro de las consideraciones sobre la confianza y la IoT, como hemos comentado en las secciones anteriores. Por ejemplo, el contexto de uso, los factores ambientales, las consideraciones de seguridad y privacidad y el historial de rendimiento de un dispositivo pueden influir en el nivel de confianza que los usuarios finales depositarán en las tecnologías de IoT. Por ejemplo, un dispositivo IoT sanitario puede requerir un mayor nivel de confianza debido a la naturaleza crítica de los datos que maneja, mientras que un dispositivo doméstico inteligente puede tener diferentes requisitos de confianza según las diferentes posibilidades, como se presenta en [41]. Comprender y adaptarse al contexto en el que se comportarán los sistemas de IoT es una parte esencial para generar y mantener la confianza entre las entidades. Además, la gestión de la confianza consciente del contexto puede ayudar a mitigar los riesgos, mejorar las experiencias de los usuarios y garantizar el funcionamiento confiable de las soluciones de IoT [79].

Todas estas definiciones están fuertemente conectadas entre sí. Así, podemos ver cómo estas conexiones pueden mejorarlas, especialmente en la confianza y el IoT, que se pueden mejorar a partir de sus implementaciones.

6 Análisis de los marcos de confianza de IoT

Como hemos propuesto en el art.5, hemos identificado seis parámetros que creemos que son importantes al considerar la confianza en IoT. En mesa2, los hemos recopilado en seis columnas. El primero está relacionado con qué tipo de modelos se han desarrollado en el trabajo seleccionado (es decir, modelo de decisión de confianza). La segunda columna contiene atributos de confianza donde se recogen las características de confianza resumidas en la Sección.5.1, métricas de confianza como la agregación de datos, actores de confianza (es decir, fideicomitente y fiduciario) y parámetros de confianza como la reputación. Luego está la Arquitectura IoT desarrollada dentro del marco seleccionado. La quinta columna está relacionada con el SDLC y si ha sido considerado en el trabajo seleccionado. Luego, están los dominios identificados por [4,5,84] relacionado con la confianza (es decir, privacidad o seguridad) y que hemos resumido en la Sección.5.2.

Tabla 2 Propiedades de las estructuras

Autores	Modelos	Atributos de confianza	Arquitectura IoT	Dominios	SDLC	Actividades
Abualese et al. [64] Ali y cols.	X		X			
[66] Bahutair et al. [76]		X	X			
Battah et al. [77] Bernabé et	X		X			X
al. [69] Bica et al. [71] De Meo	X	X	X		X	
et al. [72] Dwarakanath y	X	X	X		X	
cols. [78] Fernández-Gago et		X			X	
al. [3] Ferraris et al. [6]Fortino		X				
et al. [sesenta y cinco] Lin et	X	X	X			
al. [82] Køien [63]	X	X	X	X	X	X
	X	X	X	X	X	X
	X	X	X			
	X	X	X			
	X	X	X			
Magdich et al. [83]	X	X	X		X	X
Mahalle et al. [70]	X	X	X			
Mendoza et al. [67]		X	X			
Neisse et al. [81] Pal	X	X	X		X	X
et al. [68] Ruan et al.	X	X			X	X
[73] Ruan et al. [31]		X	X			
Saied et al. [80]	X	X		X		X
Sharma y cols. [75]	X	X	X			X
Wang y cols. [79]		X		X		
	X	X	X			X

Finalmente, en la última columna consideramos actividades que no están estrictamente relacionadas con la confianza pero que son importantes para maximizar su nivel en cada marco (es decir, trazabilidad, toma de decisiones), las hemos presentado en la Sección.5.3.

Para cada línea de la tabla2, hemos escrito el primer autor del artículo que presenta los marcos explicados en la Sección.4. En esta tabla mostramos qué trabajo cubrió los parámetros, donde se han considerado los parámetros ponemos una X. En caso contrario, el campo se deja en blanco. La tabla se encuentra en la sección Apéndice.

Para cada marco, explicaremos en detalle qué parámetros se consideran y cómo se han implementado.

6.1 Análisis de marcos

En mesa2, podemos observar la composición de los frameworks según los seis parámetros (si se consideran).

Comenzamos con un análisis genérico para comprobar los parámetros implementados en la obra. Luego, analizaremos los marcos más en detalle.

Así, podemos observar que sólo en [3] y [6] Se han considerado todos los parámetros que hemos identificado, sin embargo si entramos en detalles ambos trabajos faltan por cumplir los seis parámetros por completo. Los otros trabajos se centran sólo en varios aspectos sin considerar una arquitectura de IoT específica como en [68,71–73,75] o sin una consideración clara de los atributos de confianza [64,76]. Además, el SDLC se considera únicamente en [3,6,31, 75], pero sólo uno de ellos ha representado todas las fases [6], los otros tres implementaron sólo las primeras fases [3,31,75].

Luego, en [69], incluso si no se consideran el SDLC y las actividades relacionadas con la confianza, se han investigado todos los demás parámetros (es decir, modelos, atributos de confianza, arquitecturas de IoT y dominios relacionados con la confianza). Por otro lado, hay trabajos que consideran sólo dos parámetros, por ejemplo [64,66] o incluso solo un parámetro, por ejemplo, los atributos de confianza en [72].

En cuanto al contexto, se considera directamente en [79–81], pero es la única actividad tomada en cuenta por los mismos autores. Además, los atributos de confianza como la reputación se consideran en [67,77,79,105] o relaciones de historia pasada en [78,80,82]. Finalmente, hay algunos autores que no consideraron una especificación del modelo [66,67,71–73, 75].

A continuación presentaremos consideraciones más específicas sobre los trabajos mostrados en la Tabla2.

Comenzando con Fernández-Gago et al. [3], podemos afirmar que los autores propusieron modelos tanto de decisión como de evaluación de la confianza. Los hemos descrito en la Sección.2.2. Sin embargo, el atributo de confianza considerado es principalmente la reputación, que es el factor más importante que el tomador de decisiones tendrá en cuenta para realizar una elección entre diferentes operadores. El "ganador" es el que tiene mayor rango entre los disponibles. La arquitectura está fuertemente relacionada con el escenario. En su ejemplo, proponen un sistema compuesto por varios dispositivos IoT que se comunican con un centro central. Así, podemos definirla como una arquitectura centralizada. Sin embargo, como sugirieron los autores, también está abierto a uno distribuido. Una debilidad es que el SDLC se considera sólo para las primeras fases (es decir, requisitos, modelo y desarrollo). Aunque estas fases son fundamentales para crear el sistema adecuado, se deben tener en cuenta otras fases, como la verificación y la validación. Además, considera únicamente la privacidad y la identidad como propiedades conectadas en las que confiar. Incluso si son muy importantes, se deben tener en cuenta otros dominios, como la seguridad y la protección, para considerar el sistema de manera integral. Finalmente, podemos observar que se tiene en cuenta el contexto. Este es un parámetro muy importante, porque puede delimitar los parámetros de confianza según el contexto elegido y podemos afirmar que la confianza cambia según el contexto. Finalmente, implementan la toma de decisiones para elegir el operador más confiable para cumplir un objetivo particular.

Otro trabajo interesante es el desarrollado por Ruan et al. [31]. Este trabajo considera varias fases del SDLC y analiza la confianza con sus características y actividades relacionadas, como la toma de decisiones (que es crucial para una de las tres fases consideradas). Sin embargo, no es específico para IoT, por lo que no propone ninguna arquitectura particular y no considera ninguno de los otros dominios conectados a la confianza. Este aspecto ha sido abordado por otro trabajo del mismo autor [73] donde, aunque no se considera el SDLC y no se propone un modelo específico, se tiene en cuenta

Consideración de las diferencias entre las posibles interacciones entre los actores en un entorno de IoT. Por ejemplo, si tenemos una comunicación de dispositivo a dispositivo (D2D), las reglas y las implementaciones serán muy diferentes a las de una interacción de persona a dispositivo (H2D). Sobre los atributos de confianza, como explicamos antes, se han considerado métricas y confiabilidad. Sin embargo, este trabajo considera solo dos parámetros, pero los dos trabajos combinados pueden cubrir parcialmente todos los parámetros excepto los dominios conectados.

De manera más general, si consideramos la red de sensores inalámbricos (WSN), Ali et al. [66] han implementado un marco que considera la agregación de datos de las propiedades compuestas de confianza para crear un área confiable donde los nodos puedan intercambiar información entre ellos. Para discriminar entre nodos buenos y nodos malos, los autores implementan un modelo de amenaza bajo la perspectiva de los atacantes. Sin embargo, sin una consideración completa de otros ámbitos importantes como la seguridad, el trabajo no puede cubrir adecuadamente este aspecto.

Entonces, Pal et al. [68] consideró un aspecto importante perteneciente a una relación de confianza, especialmente para un entorno de IoT donde fusiona un sistema de recomendación directo e indirecto. Esto es útil porque es posible que dos entidades de IoT se conozcan y puedan interactuar según lo sucedido en una experiencia directa, pero también es posible que dos entidades que no se conocen quieran interactuar. En este caso deberá considerarse una confianza derivada para permitir o no este tipo de comunicaciones. Sin embargo, no presentaron una arquitectura completa y no consideraron en absoluto el SDLC.

En Ferraris et al. [6], los autores propusieron un modelo de confianza adaptativa que se explica principalmente en [41]. Este modelo es importante especialmente en un entorno doméstico inteligente, pero también se puede especificar para otros entornos (es decir, redes inteligentes), pero no para arquitecturas distribuidas. Básicamente, se divide en tres fases diferenciadas: unirse, quedarse y salir. Estas fases siempre están presentes en un entorno de IoT. En el primer caso, se realiza una decisión de confianza para los nuevos dispositivos que se unen a la red. Así, al analizar el dispositivo (es decir, reputación y problemas conocidos), otro parámetro importante que se considera es el contexto en el que se comportará al interactuar con otros dispositivos. Luego, la fase de permanencia es un seguimiento continuo del comportamiento de los dispositivos. Si una entidad de la red realizará un comportamiento sospechoso, se tomará una decisión de confianza. Esta decisión es similar al procedimiento de unión y, en caso de que produzca un resultado negativo, el dispositivo será excluido de la red o puesto en cuarentena. Finalmente, el procedimiento de baja es básicamente una desconexión de la red. Según los atributos de confianza, los autores consideran la reputación y un gran conjunto de características presentadas en la Tabla1. La arquitectura de IoT está fuertemente conectada con el modelo de confianza adaptativa discutido anteriormente. De hecho, según la decisión de confianza y la tipología del dispositivo IoT, éste puede conectarse a una red interna o externa. La red interna proporciona una mejor protección para los dispositivos IoT que tienen un poder computacional limitado. Además, el nivel de confianza de esta red es mayor que el de la red externa. En la red externa se considerarán también los dispositivos pertenecientes al paradigma Bring Your Own Device (BYOD) [106]. Sin embargo, el monitoreo de confianza es el mismo para la red interna o externa. En este trabajo se considera plenamente el SDLC desde las primeras fases del mismo hasta las finales. Así, en la fase de necesidad se analiza por qué se debería desarrollar un dispositivo IoT. Entonces,

En las fases de requisitos y modelo, se analiza estrictamente el dispositivo IoT para diseñar todas las funcionalidades e interacciones posibles. En la fase de desarrollo, estas funcionalidades se construyen y desarrollan. Luego, en las fases de verificación y validación, se realizan pruebas y comprobaciones para analizar que las funcionalidades del dispositivo IoT funcionan correctamente y reflejan su propósito previsto. Finalmente, la fase de utilización es aquella en la que el dispositivo IoT interactuará con otros dispositivos y usuarios para el propósito previsto. Los dominios analizados son una combinación de los propuestos por Hoffman y Pavlidis [4,5]. Finalmente, las actividades propuestas por este marco de IoT quieren cubrir una amplia gama de aspectos posibles. La trazabilidad permite las conexiones entre fases y entre elementos del dispositivo IoT en desarrollo. La toma de decisiones, el modelado de amenazas y la gestión de riesgos están fuertemente conectados para poder tomar decisiones de confianza. Luego, se recopila la documentación en cada fase y las puertas son las actividades que permiten la continuación del flujo durante las fases del SDLC.

En relación con el proceso de unión en una red IoT, Køien [63] propuso un modelo de confianza para la interacción entre humanos y dispositivos de IoT. Además, el autor consideró atributos de confianza como la transitividad, la integridad o la benevolencia. Según ellos, el autor fomentó los modelos Trust Network Analysis-Subjective Logic (TNA-SL) que analizan el comportamiento de una entidad en una red asimétrica donde las citas se propagan asimétricamente, así como la difusión de reputaciones/opiniones. Sin embargo, debido a que su investigación carecía de otras actividades importantes como la gestión de riesgos, inspiró a otros investigadores en esta área [107].

Acerca del SDLC, Sharma et al. [75], han presentado un marco genérico para gestionar la confianza en IoT donde se centraron especialmente en la fase de requisitos considerando parámetros cualitativos y cuantitativos, las siguientes fases son solo para el desarrollo de los requisitos. Sin embargo, incluso si el marco es interesante, tiene algunos defectos, como una retroalimentación única desde la fase final a la primera y nunca considera el contexto, que es un aspecto crucial cuando se considera la confianza y el IoT.

Por otro lado, el contexto ha sido considerado por Bahutair et al. [76]. En su trabajo, los autores consideraron un modelo de confianza adaptativo para IoT. Calcula la confiabilidad de una entidad siguiendo una arquitectura de cuatro etapas. Se trata de un trabajo interesante, con sólo algunas limitaciones dependiendo de que no considera dominios relacionados con la confianza como la seguridad, la privacidad o la identidad.

Según el marco desarrollado por Mendoza et al. [67], han considerado cómo la confianza puede ser útil utilizando protocolos de descubrimiento en una arquitectura de IoT donde los vecinos utilizan la confianza indirecta para comenzar a calcular un valor de confianza directa. Algunas desventajas son un mayor tráfico de red y consumo de energía debido al mayor intervalo de actualización; de lo contrario, este método sufrirá un diagnóstico falso retrasado durante mucho tiempo. Esto puede ser un problema en otras líneas de investigación conectadas, como la creciente IoT verde [108] paradigma. Sin embargo, su trabajo no consideró otros parámetros y probablemente la consideración del SDLC podría haber ayudado a encontrar una solución diferente con un menor consumo de energía.

Sobre el marco propuesto por Abualese et al. [64], ha considerado específicamente IoT bajo la perspectiva de Cloud of Things (CoT). Así, a partir de este punto, potenció las posibilidades de que los dispositivos IoT conectados a la nube permitan sus interacciones siguiendo reglas de modelos de decisión de confianza. Incluso si el trabajo es muy

interesante y altamente enfocado en un área particular, no considera específicamente ningún atributo de confianza, ni el SDLC, ni los dominios o actividades relacionados con la confianza. En la misma zona, Fortino et al. [sesenta y cinco] definió CoT pero desde otra perspectiva. De hecho, los autores implementaron modelos de evaluación de la confianza, especialmente considerando parámetros de reputación en lugar de modelos de decisión. Con sus experimentos, demostraron que en pequeños grupos de nodos de IoT, su algoritmo convergía rápidamente según la reputación de los agentes. Permitir que los nodos confiables traten con nodos que no son de confianza. Su enfoque considera que la confianza se calcula a partir de la reputación local. Sin embargo, no se considera SDLC, ni actividades o dominios conectados de confianza, lo que limita la contribución general.

Según los modelos de evaluación, Bica et al. [71] propuso un marco interesante que aborda la evaluación de la confianza en una arquitectura móvil considerando la seguridad y la reputación. Es valioso incluso si no es específico para IoT, pero este trabajo puede ser útil para marcos futuros que puedan implementar aspectos faltantes, como una consideración de SDLC y actividades conectadas de confianza.

Centrándose en la reputación, De Meo et al. [72] propuso un marco totalmente basado en la reputación en el que una entidad general tiene dentro un agente de reputación. Sin embargo, actúa como una entidad separada para poder evaluar el comportamiento de la entidad. Incluso si el marco considera sólo una idea general sobre cómo se pueden utilizar la confianza y la reputación, puede considerarse como un punto de partida para trabajos que consideren la raíz de la confianza [109] para dispositivos IoT.

Otro trabajo que considera importante la reputación ha sido desarrollado por Mahalle et al. [105]. Los autores realizaron un interesante análisis sobre su arquitectura de IoT. De hecho, propusieron un algoritmo para explorar nodos siguiendo sistemas de recomendación y conocimiento compartido. Por lo tanto, es posible calcular un valor de confianza para permitir que las entidades de IoT intercambien comunicaciones entre ellas. Entonces, para poder realizar esta actividad, la reputación es un parámetro fundamental según el nivel de confianza que tiene un dispositivo IoT en las demás entidades IoT conocidas. De hecho, si confían en otra entidad, pueden iniciar el cálculo de un valor de confianza siguiendo el sistema de recomendación; de lo contrario, explorarán otros nodos para calcular un valor de confianza para una entidad de IoT desconocida.

Además, la reputación ha sido considerada en el trabajo reciente desarrollado por Battah et al. [77]. Los autores propusieron una arquitectura descentralizada que también tiene en cuenta dominios relacionados con la confianza, como la privacidad y la seguridad.

En adelante, analizamos otro estudio partiendo de un enfoque completamente diferente. De hecho, Dwarakanath et al. [78] consideró solo la dependencia histórica entre dispositivos evitando el análisis de reputación. Además, restringen las posibles interacciones únicamente a H2D y D2D, evitando la consideración de H2H, porque consideran que un usuario humano, para interactuar con otro humano (bajo una perspectiva IoT), debe utilizar un dispositivo. Por tanto, para ellos, H2H es un subconjunto de D2D.

En cuanto a la toma de decisiones, un trabajo interesante es el propuesto por Bernabe et al. [69]. Los autores realizan un análisis de modelo de decisión considerando principalmente el control de acceso. Sin embargo, también implementan particularidades de los modelos de evaluación, como la reputación y las dependencias históricas entre entidades. En conexión con este aspecto, proponen una arquitectura de IoT que está fuertemente conectada con la relación social entre las entidades. Así, un dispositivo IoT perteneciente a un usuario puede confiar en otro usuario si este último tiene

una relación social con el primero. Por otro lado, si no existen relaciones sociales, los dispositivos IoT no pueden confiar en que el usuario evite la interacción. En general, podemos afirmar que ámbitos importantes como la privacidad no se consideran y creemos que, especialmente en un entorno social de IoT, se debe tener en cuenta. Sin embargo, consideran dominios importantes como la identidad y la seguridad para garantizar que las interacciones sean seguras y se realicen con entidades identificadas.

Un trabajo más reciente que propone un marco que considera la confianza en el SIoT es el presentado por Magdich et al. [83]. Se centran especialmente en aspectos de reputación. Sin embargo, consideraron por separado un parámetro importante como el contexto sólo en relación con un ataque específico (es decir, ataque de servicio oportunista (OSA)).

Según el contexto considerado, queremos destacar los trabajos de Saied et al. [80] y Wang et al. [79]. Consideran el contexto con precisión y, según él, calculan un valor de confianza diferente. Pero no consideraron otros dominios relacionados con la confianza como la privacidad o la identidad. Sin embargo, encontramos un trabajo más reciente donde Neisse et al. [81] llenar este vacío considerando algunos dominios además del contexto. Sin embargo, como mencionamos antes, creemos que también la consideración del SDLC podría haber mejorado la efectividad de estos trabajos.

Finalmente, un aspecto importante que no siempre se considera directamente en los marcos de IoT es la delegación. Lin et al. [82] definen con precisión los actores fideicomitente y fiduciario y para decidir si se puede cumplir una interacción fideicomitente-fiduciario, analizan la confiabilidad del fiduciario y la historia entre ellos. Así, si el fideicomitente confía en el fiduciario, éste puede delegar en este último la realización de una determinada actividad. Sin embargo, las interacciones se realizan sólo en un entorno SIoT.

En resumen, en la mayoría de los marcos, no se considera SDLC. Sólo varios autores lo mencionaron [3,6,75]. Creemos que esta es una fuerte limitación. De hecho, para considerar adecuadamente la confianza en el IoT, es mejor implementarlo desde las primeras fases. Además, la confianza está fuertemente relacionada con otros ámbitos como la privacidad y la seguridad. Sólo algunos artículos los consideran [3,6,68,69,77]. Esto es una debilidad, porque una consideración holística de estos dominios aumenta la confianza en un círculo virtuoso que aumenta cada uno de los dominios considerados. Luego, seis artículos evitan proponer un modelo específico [66,67,71–73, 75].

Para concluir, creemos que para considerar la confianza de manera integral en un entorno como el IoT, debemos considerar las propiedades relacionadas, el contexto y debemos planificarlo cuidadosamente a través de un SDLC completo. Hemos analizado una carencia de este aspecto en la literatura y queremos fomentar su utilización en futuros trabajos relacionados con este campo. Además, creemos que teniendo en cuenta los puntos fuertes presentados en esta encuesta, será posible crear un marco completo que pueda resultar útil para el desarrollo de dispositivos IoT. A continuación presentaremos posibles líneas de investigación que creemos que deben ser abordadas por la comunidad investigadora para considerar de manera efectiva la confianza en el IoT.

7 Retos y cuestiones abiertas

En este artículo hemos recopilado y analizado diferentes trabajos y hemos propuesto un enfoque que se debe tener en cuenta para incluir la confianza en una entidad IoT. Sin embargo, IoT y la confianza cubren aspectos diferentes y hay temas de investigación abiertos sobre estos dos temas que deben ser abordados por las comunidades de investigadores. Enumeramos a continuación aquellas que creemos que podrían ser interesantes de solucionar y abordar en el futuro:

Integración de requisitos de seguridad, confianza y reputación y metodologías modelo.

Metodologías para la obtención de requisitos de seguridad (es decir, TROPOS, Secure TROPOS, I*, TrUStAPIS [84,110–112]) se pueden fusionar para proporcionar a los desarrolladores una herramienta completa para la obtención de requisitos que conduzca a mejores prácticas bien establecidas. Esta consideración también puede ser útil para la fase de modelado, donde nuestro enfoque basado en modelos [113] y otras metodologías existentes como UMLTrust [114], o SecureUML [115] se pueden analizar juntos para explorar diferentes metodologías que pueden ser útiles en el SDLC de cualquier sistema. Investigar una forma de integrar estas metodologías para incluir seguridad, confianza y reputación puede generar un beneficio excelente para SDLC y los desarrolladores.

Configuración y soporte visual para la implementación de confianza y reputación.

Varios trabajos han propuesto soportes para que los desarrolladores o partes interesadas visualicen datos relacionados con el desarrollo de la confianza en el IoT [84,116]. De todos modos, dar pasos adicionales en esta dirección puede aumentar la productividad al centrarse en las funcionalidades centrales de una entidad de IoT confiable. También puede ser una forma de proporcionar a los desarrolladores herramientas que les ayudarán a escribir código para crear bibliotecas o marcos en una práctica conocida que se implementará durante la fase de desarrollo. Esto podría ser más efectivo si los marcos también se integraran en otras fases del SDLC para permitir una verificación automática de las entidades en desarrollo.

Creación de un modelo de confianza estándar para IoT

Con parte de nuestra investigación [117], hemos analizado los modelos de confianza de tres fabricantes diferentes (Google, Amazon, Philips), encontrando que sus modelos de confianza son muy diferentes entre ellos. Por este motivo, creemos que de acuerdo con el trabajo futuro que hemos mencionado anteriormente, es fundamental que en un futuro próximo se cree un modelo de confianza estándar para ser implementado en las entidades IoT con el fin de mejorar los aspectos de confianza y seguridad. De hecho, las diferencias entre las entidades de IoT generarán dificultades para implementar tanto la confianza como la seguridad entre las entidades y los usuarios de IoT. Si se tiene en cuenta y se desarrolla un protocolo estándar, aumentará la confianza en los dispositivos IoT y sus usuarios [43].

Confianza e Internet social de las cosas

El Internet social de las cosas (SIoT) es un nuevo concepto que vincula a las entidades de IoT y sus usuarios con las entidades de IoT y los usuarios de sus amigos, familiares o colegas. Este es un campo emergente abordado por varios autores [83,89,94, 118,119], y el concepto SIoT debe aclararse y explorarse más a fondo. Además, esta línea de investigación se puede fusionar con la anterior porque SIoT puede considerarse como bidimensional, donde también se analizan las relaciones entre usuarios.

son importantes y deben ser considerados en un modelo de confianza. Normalmente, en los paradigmas de IoT, esta dimensión no se considera. Sin embargo, en un mundo fuertemente conectado donde los usuarios tienen muchas relaciones entre ellos, este parámetro puede ser útil para desarrollar modelos de confianza que tengan en cuenta estas conexiones. Además, es necesario explorar dónde y cómo se puede aplicar SIoT tanto en el IoT profesional como en el de los consumidores. De hecho, SIoT también puede ser útil en IoT empresarial (es decir, IoT industrial [120]), especificando la interacción de las entidades y usuarios de IoT según sus funciones. Además, también se considera junto con el aprendizaje automático [121,122].

Aprendizaje automático para la computación de confianza

El aprendizaje automático ofrece una vía prometedora para abordar la incertidumbre inherente asociada a las métricas de confianza en diversos ámbitos, como las recomendaciones en línea y las redes sociales. La confianza es un concepto complejo y multifacético influenciado por factores dinámicos y dependientes del contexto. Los algoritmos de aprendizaje automático pueden ayudar a analizar grandes conjuntos de datos e identificar patrones ocultos, lo que permite predicciones de confianza más precisas y adaptables. Estos algoritmos pueden aprender de las interacciones históricas, el comportamiento del usuario y la información contextual para construir modelos de confianza más sofisticados. Además, el aprendizaje automático puede ayudar a detectar violaciones de confianza, mitigando potencialmente los riesgos asociados con actores engañosos o maliciosos. Al perfeccionar y adaptar continuamente las métricas de confianza basadas en datos en tiempo real, el aprendizaje automático proporciona una herramienta valiosa para mejorar la evaluación y gestión de la confianza en un mundo digital cada vez más interconectado.121, 122].

Ontología de confianza en el IoT

Una ontología de confianza en IoT es un marco estructurado y definido semánticamente que captura y representa el concepto complejo y multifacético de confianza dentro del ecosistema de IoT.123]. Una ontología proporciona una forma sistemática de modelar y analizar relaciones de confianza, atributos de confiabilidad y los factores que influyen en la confianza en los dispositivos de IoT. Por lo tanto, al utilizar ontologías, los sistemas de IoT pueden lograr una comprensión compartida de conceptos relacionados con la confianza y facilitar los procesos de comunicación y toma de decisiones entre varias entidades. Las ontologías de confianza ayudan a estandarizar la representación de datos de confianza, facilitando el intercambio e integración de información sobre la confiabilidad de las entidades de IoT. Pueden servir como una herramienta importante para desarrollar sistemas de gestión de confianza adaptables y conscientes del contexto que mejoren la seguridad, confiabilidad y transparencia de los entornos de IoT.

IoT verde y confianza

Otro tema importante que debe abordar la comunidad investigadora está relacionado con el consumo de eficiencia energética de los dispositivos IoT. El creciente número de dispositivos se convertirá en un problema de consumo de energía. Por tanto, será fundamental garantizar la confianza teniendo en cuenta también el aspecto energético. Varios autores [108,124–126] ya han comenzado a investigar este campo, pero la comunidad investigadora debería considerarlo en un futuro próximo, con el fin de proporcionar un entorno de IoT sostenible para el planeta. El IoT verde puede traer cambios importantes en el mundo ayudando a reducir el efecto invernadero permitiendo un mundo sostenible.

8 Conclusión

En este artículo hemos profundizado en cómo la confianza y el IoT han sido presentados en el estado del arte por diferentes autores. Incluso si se han realizado investigaciones en los campos de la confianza y la IoT, es necesario mejorar este esfuerzo. Hemos analizado trabajos en los que la confianza y el IoT se han considerado juntos centrándonos en los marcos para la confianza y el IoT. Analizándolos, hemos clasificado varios parámetros que creemos que son fundamentales, como el SDLC, los dominios conectados a la confianza y las diferentes características de la confianza. Así, hemos recopilado los trabajos identificados que destacan qué parámetros se consideran y cuáles faltan para proporcionar una guía novedosa para considerar adecuadamente la confianza en IoT. Finalmente, hemos proporcionado una serie de desafíos y cuestiones abiertas que, en nuestra opinión, deberían ser abordadas por la comunidad investigadora.

Para trabajos futuros, seguiremos las pautas propuestas en esta encuesta para proporcionar un marco completo de gestión de confianza. Además, contribuiremos con los desafíos propuestos al final del artículo. De hecho, creemos que estos problemas deben abordarse y resolverse para mejorar el entorno de IoT.

AgradecimientosEste trabajo ha sido parcialmente apoyado por los proyectos: BIGPrivDATA (UMA20-FEDERJA-082) del Programa FEDER Andalucía 2014-2020. Además, agradecemos a Huawei Technologies por su apoyo.

Contribuciones de autor Los autores contribuyeron igualmente a este trabajo.

FondosFinanciación para publicación en acceso abierto: Universidad Málaga/CBUA.

Disponibilidad de datos y materiales. No aplica.

Declaraciones

Conflicto de intereses No aplica.

Aprobación ética No aplica.

Referencias

1. Roman R, Najera P, Lopez J (2011) Asegurar el Internet de las cosas. Computadora 44(9):51–58
2. Čolaković A, Hadžialić M (2018) Internet de las cosas (IoT): una revisión de las tecnologías habilitadoras, los desafíos y las cuestiones de investigación abiertas. Red informática 144: 17–39

3. Fernández-Gago C, Moyano F, López J (2017) Modelado de dinámicas de confianza en Internet de las cosas. Ciencia informática 396:72–82
4. Hoffman LJ, Lawson-Jenkins K, Blum J (2006) Confianza más allá de la seguridad: un modelo de confianza ampliado. Común ACM 49(7):94–101
5. Pavlidis M, Diseñar para la confianza (2011) CAiSE (Consorcio Doctoral), págs. 3–14
6. Ferraris D, Fernández-Gago C, López J (2018) Un marco de confianza por diseño para Internet de las cosas. En: Vía de seguridad NTMS'2018 (vía de seguridad NTMS 2018), págs. 1–4
7. Mohammadi V, Rahmani AM, Darwesh AM, Sahafi A (2019) Sistemas de recomendación basados en la confianza en Internet de las cosas: una revisión sistemática de la literatura. HCIS 9(1):1–61
8. Levien RL (2002) Métricas de confianza resistentes a ataques. Doctor. tesis, Universidad de California en Berkeley
9. Grandison T, Sloman M (2000) Una encuesta sobre la confianza en las aplicaciones de Internet. Tutor de supervivencia comunitaria IEEE 3(4):2–16
10. Aaqib M, Ali A, Chen L, Nibouche O (2023) Mucha confianza y reputación: una encuesta y una taxonomía. J Computación en la nube 12(1):1–20
11. Altaf A, Abbas H, Iqbal F, Derhab A (2019) Modelos confiables de Internet de cosas inteligentes: una encuesta, cuestiones abiertas y direcciones futuras. Aplicación J Netw Comput 137:93–111
12. Fotia L, Delicato F, Fortino G (2023) Confianza en las arquitecturas de Internet de las cosas basadas en el borde: estado del arte y desafíos de investigación. Encuesta informática ACM 55(9):1–34
13. Guo J, Chen R, Tsai J (2017) Una encuesta sobre modelos de cálculo de confianza para la gestión de servicios en sistemas de Internet de las cosas. Computación Comunitaria 97:1–14
14. Marsh SP (1994) Formalizar la confianza como concepto computacional. Doctor. Tesis, Departamento de Ciencias de la Computación y Matemáticas, Universidad de Stirling
15. Yan Z, Holtmanns S (2008) Modelado y gestión de la confianza: de la confianza social a la confianza digital. Globo IGI 290–323
16. Erickson J, (2009) Métricas de confianza. En: Tecnologías y sistemas colaborativos, CTS'09, simposio internacional, págs. 93–97
17. McKnight DH, Chervany NL (2000) ¿Qué es la confianza? Un análisis conceptual y un modelo interdisciplinario. En: Actas AMCIS 2000, vol 382, págs. 827–833
18. Mayer Roger C., Davis James H., Schoorman F. David (1995) Un modelo integrador de confianza organizacional. Acad Manag Rev. 20(3):709.https://doi.org/10.2307/258792
19. McKnight DH, Chervany NL (1996) Los significados de la confianza, Informe técnico Serie de documentos de trabajo MISRC 96-04
20. Gambetta D (2000) ¿Podemos confiar en la confianza? En: Creación y ruptura de relaciones cooperativas de confianza, vol 13, págs. 213–237
21. Mui L, Mohtashemi M, Halberstadt A (2002) Un modelo computacional de confianza y reputación. En: Actas de la 35ª Conferencia Internacional Anual de Hawaii sobre Ciencias de Sistemas, 2002. HICSS. IEEE, págs. 2431–2439
22. Ruohomaa S, Kutvonen L (2005) Encuesta sobre gestión de confianza. En: Congreso Internacional sobre Gestión Fiduciaria. Springer, págs. 77–92
23. Jøsang A, Ismail R, Boyd C (2007) Una encuesta sobre sistemas de confianza y reputación para la prestación de servicios en línea. Sistema de soporte Decis 43(2):618–644
24. Agudo I, Fernández-Gago C, López J (2008) Un modelo para el análisis de métricas de confianza. En: Conferencia Internacional sobre Confianza, Privacidad y Seguridad en los Negocios Digitales. Springer, págs. 28-37
25. Olmedilla D, Rana OF, Matthews B, Nejdl W (2006) Problemas de seguridad y confianza en redes semánticas. En: Actas del seminario Dagstuhl, Schloss Dagstuhl – Leibniz – Zentrum für Informatik, págs. 1–11
26. Moyano F, Fernández-Gago C, López J (2012) Un marco conceptual para modelos de confianza. En: Novena Conferencia Internacional sobre Confianza, Privacidad y Seguridad en los Negocios Digitales (TrustBus 2012, vol 7449 de Lectures Notes in Computer Science. Springer, págs. 93-104
27. Cofta P (2007) Confianza, confianza e identidad. BT Technol J 25(2):173–178
28. Cofta P (2007) Confianza, complejidad y control: confianza en un mundo convergente. Wiley, Nueva York
29. Miller KW, Voas J (2009) La metafísica de la confianza en el software. Profesor de TI 11(2):52–55
30. Marsh S, Dibben MR (2005) Confianza, desconfianza, desconfianza y desconfianza: una exploración del lado (más) oscuro. En: Congreso Internacional sobre Gestión Fiduciaria. Springer, págs. 17-33
31. Ruan Y, Durresi A (2016) Una encuesta sobre sistemas de gestión de confianza para comunidades sociales en línea modelado de confianza, inferencia de confianza y ataques. Sistema basado en el conocimiento 106:150–163
32. Louta M, Michalas A (2010) Hacia marcos de mercado electrónico eficientes y conscientes de la confianza. En: Enciclopedia sobre el desarrollo y la gestión del comercio electrónico en la economía global, págs. 273–283

33. Blaze M, Feigenbaum J, Lacy J (1996) Gestión de confianza descentralizada. En: Procedimientos de privacidad y seguridad del simposio IEEE, págs. 164-173
34. Beth T, Borcherding M, Klein B (1994) Valoración de la confianza en redes abiertas. En: Simposio europeo sobre investigación en seguridad informática. Springer, págs. 1-18
35. Winslett M, Yu T, Seamons KE, Hess A, Jacobson J, Jarvis R, Smith B, Yu L (2002) Negociar la confianza en la web. Computación de Internet IEEE 6 (6): 30–37
36. Watson DS, Piette MA, Sezgen O, Motegi N, Ten Hope L (2004) Tecnología de máquina a máquina (m2m) en edificios comerciales que responden a la demanda
37. Gazis V (2016) Un estudio de estándares para máquina a máquina e Internet de las cosas. Tutor de supervivencia comunitaria IEEE 19(1):482–511
38. Pei Z, Deng Z, Yang B, Cheng X (2008) Plataformas de hardware y protocolos de comunicación de redes de sensores inalámbricos orientados a aplicaciones: una encuesta, Tecnología industrial. En: Conferencia Internacional IEEE, págs. 1–6
39. Gill K, Yang SH, Yao F, Lu X (2009) Un sistema de automatización del hogar basado en zigbee, IEEE, Transacciones sobre el consumidor. Electrónica 55(2):422–430
40. Bronzi W, Frank R, Castignani G, Engel T (2026) Análisis de robustez y rendimiento de baja energía de Bluetooth para comunicaciones entre vehículos. Red ad hoc 37:76–86
41. Ferraris D, Fernández-Gago C, Daniel J, López J (2019) Una arquitectura segregada para una red de Internet de las cosas basada en la confianza. En: 16ª Conferencia Anual de Redes y Comunicaciones del Consumidor (CCNC) del IEEE, págs. 1–6
42. Singh S, Sharma PK, Park JH (2017) Sh-secnet: una arquitectura de red segura mejorada para el diagnóstico de amenazas a la seguridad en un hogar inteligente. Sostenibilidad 9(4):1–19
43. Roman R, Zhou J, Lopez J (2013) Sobre las características y desafíos de la seguridad y la privacidad en la Internet distribuida de las cosas. Red informática 57(10):2266–2279
44. Dohr A, Modre-Opsrian R, Drobics M, Hayn D, Schreier G (2010) Internet de las cosas para una vida asistida por ambiente. En: 2010 Séptima Conferencia Internacional Tecnología de la Información: Nuevas Generaciones (ITNG), págs. 804–809
45. Parra J, Hossain MA, Uribarren A, Jacob E, El Saddik A (2009) Arquitectura doméstica inteligente flexible que utiliza el perfil del dispositivo para servicios web: un enfoque de igual a igual. Int J Hogar inteligente 3(2):39–56
46. BlR Stojkoska, Trivodaliev KV (2017) Una revisión del Internet de las cosas para el hogar inteligente: desafíos y soluciones. J Producto limpio 140:1454–1464
47. Stouffer K, Falco J, Scarone K (2011) Guía de seguridad de sistemas de control industrial (ICS). Publicación de especificaciones NIST 800(82)
48. Porambage P, Ylianttila M, Schmitt C, Kumar P, Gurtov A, Vasilakos AV (2016) La búsqueda de la privacidad en Internet de las cosas. Computación en la nube IEEE 3 (2): 36–45
49. Leister W, Schulz T (2012) Ideas para un indicador de confianza en Internet de las cosas. INTELIGENTE 12:31–34
50. Azzedin F, Ghaleb M (2019) Internet de las cosas y fusión de información: encuesta sobre la perspectiva de la confianza. Sensores 19(8):1929
51. Elkhodr M, Alsinglawi B (2019) Procedencia de los datos y establecimiento de confianza en Internet de las cosas. Privacidad segura e99
52. Yan Z, Zhang P, Vasilakos AV (2014) Una encuesta sobre gestión de confianza para Internet de las cosas. Aplicación J Netw Comput 42:120–134
53. Masthoff J (2007) Modelado computacional de la confianza: una exploración. En: Actas del taller SociUM asociado con la Conferencia de modelado de usuarios, págs. 1–10
54. Wang EK, Chen CM, Zhao D, Ip WH, Yung KL (2019) Un modelo de confianza dinámico en Internet de las cosas. Computación suave 1–10
55. Hussain Y, Zhiqiu H, Akbar MA, Alsanad A, Alsanad AA-A, Nawaz A, Khan IA, Khan ZU (2020) Modelo de reputación y confianza contextual para IoT basado en niebla. Acceso IEEE 8:31622–31632
56. Ursino D, Virgili L (2020) Un enfoque para evaluar la confianza y la reputación de las cosas en un escenario de múltiples iots. Computación 102 (10): 2257–2298
57. Li N, Varadharajan V, Nepal S (2019) Sistema de gestión de confianza contextual para aplicaciones iot con múltiples dominios. En: IEEE 39.ª Conferencia Internacional sobre Sistemas de Computación Distribuida (ICDCS), págs. 1138–1148
58. Fortino G, Fotia L, Messina F, Rosaci D, Sarné GM (2019) Un mecanismo de reputación para apoyar la cooperación de dispositivos iot, IA e IoT celebrado conjuntamente con AI* IA 2019. En: La 18.ª Conferencia Internacional de la Asociación Italiana para Inteligencia Artificial, CEUR, págs. 1-12
59. Fortino G, Fotia L, Messina F, Rosaci D, Sarné GM (2020) Confianza y reputación en Internet de las cosas: estado del arte y desafíos de investigación. Acceso IEEE 8:60117–60125

60. Sadique KM, Rahmani R, Johannesson P (2018) Confianza en Internet de las cosas: una arquitectura para la futura red iot. En: Conferencia Internacional sobre Innovación en Ingeniería y Tecnología (ICIET), págs. 1–5
61. Junejo AK, Komninos N, Sathiyanarayanan M, Chowdhry BS (2019) Fideicomisario: un sistema de gestión de confianza para sistemas ciberfísicos habilitados para niebla. IEEE Trans Emerg Top Computadora 9(4):2030–2041
62. Alemneh E, Senouci SM, Brunet P, Tegegne T (2020) Un sistema de gestión de confianza bidireccional para computación en la niebla. Sistema informático Futur Gener 106:206–220
63. Køien GM (2011) Reflexiones sobre la confianza en los dispositivos: una encuesta informal sobre la confianza humana en un contexto de Internet de las cosas. Wirel Pers Commun 61(3):495–510
64. Abualese H, Al-Rousan T, Al-Shargabi B (2019) Un nuevo marco de confianza para el gobierno electrónico en la nube de cosas. Int J Electron Telecommun 65
65. Fortino G, Messina F, Rosaci D, Sarné GM (2018) Uso de la confianza y la reputación local para la formación de grupos en la nube de las cosas. Sistema de Computación Futur Gener 89:804–815
66. Ali BA, Abdulsalam HM, AlGhemlas A (2018) Esquema basado en confianza para redes de sensores inalámbricos habilitadas para iot. Comunicaciones personales inalámbricas 99(2):1061–1080
67. Mendoza CV, Kleinschmidt JH (2018) Un mecanismo de gestión de confianza distribuida para Internet de las cosas utilizando un enfoque multiservicio. Persona de Wirel Commun 103(3):2501–2513
68. Pal S, Hitchens M, Varadharajan V (2019) Hacia el diseño de un marco de gestión de confianza para Internet de las cosas. En: 13.ª Conferencia Internacional sobre Tecnología de Sensores (ICST), págs. 1–7
69. Bernabe JB, JlH Ramos, Gomez AFS (2016) Taciot: sistema de control de acceso multidimensional consciente de la confianza para el Internet de las cosas. Computación blanda 20 (5): 1763–1779
70. Mahalle PN, Thakre PA, Prasad NR, Prasad R (2013) Un enfoque difuso para el control de acceso basado en la confianza en Internet de las cosas. En: VITAE IEEE inalámbrico, págs. 1 a 5
71. Bica I, Chifor BC, Arseni SC, Matei I (2019) Marco de seguridad basado en reputación para Internet de las cosas. En: Conferencia Internacional sobre Seguridad de las Tecnologías de la Información y las Comunicaciones. Springer, págs. 213-226
72. De Meo P, Messina F, Postorino MN, Rosaci D, Sarné GM (2017) Un marco de reputación para compartir recursos en entornos basados en iot. En: 14.ª Conferencia Internacional del IEEE sobre redes, detección y control (ICNSC) de 2017, págs. 513–518
73. Ruan Y, Durresi A, Alfantoukh L (2016) Marco de gestión de confianza para Internet de las cosas. En: Conferencia internacional IEEE Aplicaciones y redes de información avanzadas (AINA), págs. 1013-1019
74. Hand DJ (1996) La estadística y la teoría de la medición. J Roy Stat Soc Ser A (Stat Soc) 445–492
75. Sharma A, Pilli ES, Mazumdar AP, Govil M (2016) Un marco para gestionar la confianza en Internet de las cosas. En: Conferencia Internacional Tendencias Emergentes en Tecnologías de la Comunicación (ETCT). IEEE, págs. 1 a 5
76. Bahutair M, Bougeuttaya A, Neiat AG (2019) Confianza adaptativa: confianza basada en el uso en servicios de IoT de colaboración colectiva. En: Conferencia internacional IEEE sobre servicios web (ICWS), págs. 172-179
77. Battah AA, Iraqi Y, Damiani E (2022) Un sistema de confianza y reputación para interacciones de servicios de IoT. IEEE Trans Netw Serv Administrar 19(3):2987–3005
78. Dwarakanath R, Koldehofe B, Bharadwaj Y, Nguyen TAB, Eyers D, Steinmetz R (2017) Trustcep: adopción de un enfoque basado en la confianza para el procesamiento distribuido de eventos complejos. En: 18ª Conferencia Internacional IEEE sobre Gestión de Datos Móviles (MDM), págs. 30–39
79. Wang Y, Chen R, Cho JH, Swami A, Lu YC, Lu CT, Tsai JJ (2016) Catrust: gestión de confianza contextual para redes ad hoc orientadas a servicios. Computación IEEE Trans Serv 11(6):908–921
80. Saied YB, Olivereau A, Zeghlache D, Laurent M (2013) Diseño de sistemas de gestión de confianza para Internet de las cosas: un enfoque multiservicio y consciente del contexto. Seguridad informática 39:351–365
81. Neisse R, Steri G, Baldini G, Tragos E, Fovino IN, Botterman M (2022) Marco de privacidad y seguridad de IoT dinámico, escalable y basado en la confianza, consciente del contexto. En: Aplicaciones de Internet de las cosas: desde la investigación y la innovación hasta el despliegue en el mercado. Editores del río, págs. 199–224
82. Lin Z, Dong L (2017) Aclarar la confianza en el Internet social de las cosas. IEEE Trans Knowl Data Eng 30(2):234–248
83. Magdich R, Jemal H, Ayed MB (2022) Un marco de gestión de confianza resiliente frente a ataques relacionados con la confianza en el Internet social de las cosas. Computación comunitaria 191: 92–107
84. Ferraris D, Fernández-Gago C (2020) Trustapis: un método de obtención de requisitos de confianza para iot. Int J Inf Secur 19(1):111–127

85. Ferraris D, Fernandez-Gago C, Lopez J (2022) Enfoques novedosos para el desarrollo de entidades IoT confiables. En: Conferencia internacional IFIP sobre seguridad de sistemas TIC y protección de la privacidad, págs. 215–230

86. Ferraris D, Fernández-Gago C, López J (2022) Métodos de verificación y validación para un marco de confianza por diseño para IoT. En: Conferencia anual de IFIP sobre seguridad y privacidad de datos y aplicaciones, págs. 183–194

87. Nguyen J, Dupuis M (2019) Cerrar el ciclo de retroalimentación entre el diseño de UX, el desarrollo de software, la ingeniería de seguridad y las operaciones. En: Actas de la 20ª Conferencia Anual SIG sobre Educación en Tecnología de la Información, págs. 93–98

88. Chen L (2015) Entrega continua: enormes beneficios, pero también desafíos. Software IEEE 32(2):50–54

89. Abdelghani W, Zayani CA, Amous I, Sèdes F (2016) Gestión de la confianza en el Internet social de las cosas: una encuesta. En: Jornada sobre e-Business, e-Servicios y e-Sociedad. Springer, págs. 430–441

90. Christianson B, Harbison WS (1996) ¿Por qué la confianza no es transitiva? Taller internacional sobre protocolos de seguridad. Springer, págs. 171-176

91. Chang J, Wang H, Gang Y (2006) Una métrica de confianza dinámica para sistemas p2p. En: Quinta Conferencia Internacional sobre Talleres de Computación Grid y Cooperativa. IEEE, págs. 117-120

92. Kenning P (2008) La influencia de la confianza general y la confianza específica en el comportamiento de compra. Gestión de distribución minorista internacional J 36 (6): 461–476

93. Morrow Jr J, Hansen MH, Pearson AW (2004) Los antecedentes cognitivos y afectivos de la confianza general dentro de las organizaciones cooperativas. J Manag Números 48 a 64

94. Nitti M, Girau R, Atzori L (2014) Gestión de la confiabilidad en el Internet social de las cosas. IEEE Trans Knowl Data Eng 26(5):1253–1266

95. Presti SL, Butler M, Leuschel M, Booth C (2007) Diseño de confianza holístico de servicios electrónicos. En: Confianza en los servicios electrónicos: tecnologías, prácticas y desafíos. IGI Global, págs. 113-139

96. Núñez D et al. (2013) D: C-5.1 métricas de rendición de cuentas. Entregable del proyecto D 35

97. Stapelberg RF (2009) Manual de confiabilidad, disponibilidad, mantenibilidad y seguridad en el diseño de ingeniería. Springer, Berlín

98. Ferraris D, Fernandez-Gago C, Lopez J (2023) POM: una metodología similar a ahp basada en la confianza para resolver requisitos de conflicto para IoT. En: Enfoques colaborativos para la seguridad cibernética en sistemas ciberfísicos, págs. 145-170

99. Lăzăroiu G, Neguriţă O, Grecu I, Grecu G, Mitran PC (2020) Proceso de toma de decisiones de los consumidores en plataformas de comercio social: confianza en línea, riesgo percibido e intenciones de compra. Psicología frontal 11:890

100. Matzembacher DE, do Carmo Stangherlin I, Slongo LA, Cataldi R (2018) Una integración de elementos de trazabilidad y su impacto en la confianza del consumidor. Control de alimentos 92:420–429

101. Steinauer DD, Wakid SA, Rasberry S (1997) Confianza y trazabilidad en el comercio electrónico. Vista del stand 5(3):118–124

102. Dimitrakos T, Dilshener T, Kravtsov A, La Marra A, Martinelli F, Rizos A, Rosetti A, Saracino A (2020) Autorización continua consciente de la confianza para una confianza cero en el Internet de las cosas del consumidor. En: IEEE 19.ª Conferencia Internacional sobre Confianza, Seguridad y Privacidad en la Computación y las Comunicaciones (TrustCom), págs. 1801–1812

103. Zheng D, Luo Q, Ritchie BW (2022) El papel de la confianza en la mitigación de la amenaza percibida, el miedo y la evitación de viajes después de un brote pandémico: un análisis multigrupo. J Viajes Res 61(3):581–596

104. Saaty TL (2008) Toma de decisiones con el proceso de jerarquía analítica. Int J Serv Ciencia 1(1):83–98

105. Mahalle P, Babar S, Prasad NR, Prasad R (2010) Marco de gestión de identidad hacia Internet de las cosas (iot): hoja de ruta y desafíos clave. En: Conferencia internacional sobre aplicaciones y seguridad de redes. Springer, págs. 430–439

106. Miller KW, Voas J, Hurlburt GF (2012) Byod: consideraciones de seguridad y privacidad. Profesor 14(5):53–55

107. Thapa SJ (2021) Comprensión de los riesgos de seguridad y la percepción de los usuarios sobre la adopción de dispositivos portátiles. Cosas médicas de Internet

108. Khan ZA (2018) Uso de una gestión de confianza energéticamente eficiente para proteger las redes de iot para ciudades inteligentes. Sostener las ciudades Soc. 40:1–15

109. Zhao S, Zhang Q, Hu G, Qin Y, Feng D (2014) Proporcionar una raíz de confianza para ARM TrustZone mediante SRAM en chip. En: Actas del cuarto taller internacional sobre dispositivos integrados confiables, págs. 25–36

110. Bresciani P, Perini A, Giorgini P, Giunchiglia F, Mylopoulos J (2004) Tropos: una metodología de desarrollo de software orientada a agentes. Sistema multiagente de agente automático 8(3):203–236

111. Mouratidis H, Giorgini P (2007) Tropos seguros: una extensión orientada a la seguridad de la metodología tropos. Int J Software Eng Knowl Eng 17(02):285–309
112. Yu E, Liu L (2001) Modelado de confianza para el diseño de sistemas utilizando el marco de actores estratégicos i*. En: Confianza en las cibersociedades. Springer, págs. 175-194
113. Ferraris D, Fernández-Gago C, López J (2020) Un enfoque basado en modelos para garantizar la confianza en IoT. HCIS 10:1–33
114. Uddin MG, Zulkernine M (2008) Umltrust: hacia el desarrollo de software consciente de la confianza. En: Actas del simposio ACM de 2008 sobre informática aplicada. ACM, págs. 831–836
115. Lodderstedt T, Basin D, Doser J (2002) Secureuml: un lenguaje de modelado basado en uml para seguridad basada en modelos. En: Conferencia internacional sobre el lenguaje de modelado unificado. Springer, págs. 426–441
116. Mavropoulos O, Mouratidis H, Fish A, Panaousis E, Kalloniatis C (2016) Aparato: razonamiento sobre los requisitos de seguridad en Internet de las cosas. En: Congreso Internacional sobre Ingeniería de Sistemas de Información Avanzados. Springer, págs. 219-230
117. Ferraris D, Bastos D, Fernandez-Gago C, El-Moussa F (2020) Un modelo de confianza para dispositivos domésticos inteligentes populares. Int J Inf Secur 1–17
118. Atzori L, Iera A, Morabito G, Nitti M (2012) 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. Red informática 56(16):3594–3608
119. Sharma V, You I, Jayakody DNK, Atiquzzaman M (2019) Transmisión cooperativa de confianza y preservación de la privacidad a través del crowdsourcing en el Internet social de las cosas. Sistema de Computación Futur Gener 92:758–776
120. Wang J, Wang M, Zhang Z, Zhu H (2022) Hacia un marco de evaluación de confianza contra comportamientos maliciosos de la IoT industrial. Cosas de Internet del IEEE J 9(21):21260–21277
121. Ali-Eldin AM (2022) Un enfoque híbrido de computación de confianza para IoT que utiliza similitud social y aprendizaje automático. MÁS UNO 17(7):e0265658
122. Sagar S, Mahmood A, Sheng QZ, Zhang WE (2020) Heurística computacional de confianza para el Internet social de las cosas: un enfoque basado en el aprendizaje automático. En: ICC 2020-2020 Conferencia Internacional de Comunicaciones (ICC) del IEEE, págs. 1–6
123. Kotis K, Katasonov A (2012) Una ontología para la implementación automatizada de aplicaciones en entornos de IoT heterogéneos. Web semántica J (SWJ)
124. Sharma PK, Kumar N, Park JH (2020) Tecnología Blockchain hacia la IoT verde: oportunidades y desafíos. Red IEEE 34(4):263–269
125. Hellaoui H, Koudil M, Bouabdallah A (2020) Eficiencia energética en la seguridad de la iot basada en 5g: un enfoque adaptativo de extremo a extremo. Cosas de Internet del IEEE J 7(7):6589–6602
126. Ilyas M, Ullah Z, Khan FA, Chaudary MH, Malik MSA, Zaheer Z, Durrani HUR (2020) Protocolo de enrutamiento energéticamente eficiente basado en confianza para redes de sensores basadas en Internet de las cosas. Red de sensor de distribución J int 16(10):1–20