

SERVICIO DE SEGURIDAD DEL INTERNET DE LAS COSAS

Antecedentes de la invención

El internet de las cosas (IoT, por sus siglas en inglés) generalmente se refiere a un sistema de dispositivos capaces de comunicarse a través de una red. Los dispositivos pueden incluir objetos cotidianos como tostadoras, cafeteras, sistemas termostáticos, lavadoras, secadoras, lámparas, automóviles y similares. Las comunicaciones de red pueden utilizarse para la automatización de dispositivos, captura de datos, suministro de alertas, personalización de configuraciones y muchas otras aplicaciones.

Breve descripción de la invención

Esta breve descripción de la invención se proporciona para introducir una selección de conceptos en una forma simplificada que se aborda con más detalle a continuación en la descripción detallada. Esta breve descripción de la invención no tiene la intención de identificar características importantes o características esenciales de la materia objeto reivindicada, ni pretende utilizarse para limitar el alcance de la materia objeto reivindicada.

En pocas palabras, la tecnología divulgada se dirige generalmente a la seguridad del dispositivo en un entorno de IoT. Por ejemplo, tal tecnología es utilizable en la seguridad de IoT. En un ejemplo de la tecnología, se almacena un conjunto de reglas de seguridad que están asociadas con una condición esperada de al menos un dispositivo de IoT. Se reciben los datos de IoT asociados con al menos un dispositivo de IoT. Los datos de IoT pueden ser datos agregados que incluyen al menos dos tipos diferentes de datos. Se realiza una determinación, con base en los datos de IoT, en cuanto a si el conjunto de reglas de seguridad se infringió. Una alerta se envía de forma selectiva con base en la determinación.

Algunos ejemplos de la divulgación incluyen un sistema para monitorizar, detectar y disminuir las amenazas de seguridad para los dispositivos de IoT utilizando la telemetría sobre el estado de seguridad del dispositivo de IoT, y utilizando otros datos del entorno a partir de otros dispositivos de IoT. En algunos ejemplos, se utilizan los datos de telemetría de múltiples dispositivos de IoT en el entorno, y se forma un modelo resultante del entorno. En algunos ejemplos, el modelo resultante se utiliza para detectar las amenazas de seguridad como intrusiones y manipulación.

Otros aspectos y aplicaciones de la tecnología divulgada se apreciarán tras leer y comprender las figuras adjuntas y la descripción.

Breve descripción de los dibujos

Los ejemplos no limitativos ni exhaustivos de la presente divulgación se describen con referencia a los siguientes dibujos. En los dibujos, los números de referencia similares se refieren a partes similares en las distintas figuras, a menos que se especifique lo contrario. Estos dibujos no están necesariamente representados a escala.

Para una mejor comprensión de la presente divulgación, se hará referencia a la siguiente descripción detallada, que debe leerse en asociación con los dibujos adjuntos, en los cuales:

La figura 1 es un diagrama de bloques que ilustra un ejemplo de un entorno adecuado en el cual pueden emplearse aspectos de la tecnología;

La figura 2 es un diagrama de bloques que ilustra un ejemplo de un dispositivo informático adecuado de acuerdo con los aspectos de la tecnología descrita;

La figura 3 es un diagrama de bloques que ilustra un ejemplo de un sistema para la seguridad de IoT;

La figura 4 es un diagrama que ilustra un flujo de datos ejemplar para un proceso de seguridad de IoT; y

La figura 5 es un diagrama de flujo lógico que ilustra un ejemplo de un proceso para la seguridad de IoT, de acuerdo con aspectos de la presente divulgación.

Descripción detallada de la invención

La siguiente descripción proporciona detalles específicos para una completa comprensión y habilitación de la descripción de varios ejemplos de la tecnología. Un experto en la técnica entenderá que la tecnología puede practicarse sin muchos de estos detalles. En algunos casos, las estructuras y funciones bien conocidas no se han mostrado o descrito en detalle para evitar hacer confusa innecesariamente la descripción de los ejemplos de la tecnología. Se pretende que la terminología utilizada en esta divulgación se interprete de la manera más amplia y razonable posible, aunque se utilice junto con una descripción detallada de ciertos ejemplos de la tecnología. Aunque algunos términos pueden enfatizarse a continuación, cualquier terminología que se intente interpretar de manera restringida se definirá de manera clara y específica como tal en esta sección de la descripción detallada. A lo largo de la especificación y reivindicaciones, los siguientes términos adquieren al menos los significados explícitamente asociados en el presente documento, a menos que el contexto indique lo contrario. Los significados identificados a continuación no limitan necesariamente los términos, sino que simplemente proporcionan ejemplos ilustrativos de los términos. Por ejemplo, cada uno de los términos “con base en” y “basado en” no es exclusivo, y es equivalente al término “con base, al menos en parte, en”, e incluye la opción de basarse en factores adicionales, algunos de ellos pueden no describirse en el presente documento. Como otro ejemplo, el término “a través de” no es exclusivo, y es equivalente al término “a través, al menos en parte, de”, e incluye la opción de ser a través de factores adicionales, algunos de los cuales pueden no describirse en el presente documento. El significado de “en” incluye “en” y “sobre”. La frase “en una modalidad” o “en un ejemplo”, tal como se utiliza en el presente documento, no se refiere necesariamente a la misma modalidad o ejemplo, aunque puede ser así. El uso de designadores numéricos textuales particulares no implica la existencia de designadores numéricos de menor valor. Por ejemplo, mencionar “una miniaplicación seleccionada del grupo que consiste en una tercera *foo* y una cuarta *bar*” no implicaría en sí mismo que exista al menos tres *foo*, ni que exista al menos cuatro *bar*. Las referencias en singular se hacen meramente por claridad de lectura e incluyen

referencias plurales a menos que se excluyan específicamente las referencias plurales. El término “o” es un operador inclusivo “o” a menos que se indique específicamente lo contrario. Por ejemplo, las frases “A o B” significa “A, B, o A y B”. Tal como se utiliza en el presente documento, los términos “componente” y “sistema” pretenden abarcar *hardware*, *software* o varias combinaciones de *hardware* y *software*. Así, por ejemplo, un sistema o componente puede ser un proceso, un proceso que se ejecuta en un dispositivo informático, el dispositivo informático, o una porción del mismo. El término “concentrador de IoT” no se limita a un tipo particular de servicio de IoT, sino que se refiere al dispositivo con el cual se comunica el dispositivo de IoT, después del aprovisionamiento, para al menos una solución de IoT o un servicio de IoT de cualquier tipo. Es decir, el término “concentrador de IoT”, tal como se utiliza en toda la especificación y las reivindicaciones, es genérico para cualquier solución de IoT.

En pocas palabras, la tecnología divulgada generalmente se dirige a la seguridad del dispositivo en un entorno de IoT. Por ejemplo, esta tecnología es utilizable en la seguridad de IoT. En un ejemplo de la tecnología, se almacena un conjunto de reglas de seguridad asociadas con una condición esperada de al menos un dispositivo de IoT. Se reciben los datos de IoT asociados con al menos un dispositivo de IoT. Los datos de IoT pueden ser datos agregados que incluyen al menos dos tipos diferentes de datos. Se realiza una determinación, con base en los datos de IoT, en cuanto a si el conjunto de reglas de seguridad se infringió. Una alerta se envía de forma selectiva con base en la determinación.

En algunas aplicaciones, los dispositivos de IoT tienden a implementarse de forma remota, potencialmente en entornos adversos. Con frecuencia, tales dispositivos pueden no ser físicamente accesibles para los operadores o propietarios del dispositivo. Tales dispositivos también pueden encontrarse “libremente” para que estén desatendidos y físicamente disponibles para el público sin monitorización física, supervisión física o seguridad física, y así las personas pueden manipular físicamente los dispositivos. Puede ser posible que alguien transfiera programas maliciosos a un dispositivo de este tipo, robe un certificado de tal dispositivo o similar. Los ejemplos de la divulgación monitorizan la seguridad de los dispositivos, detectan intrusiones y/o amenazas al dispositivo y/o comunican tales intrusiones y/o amenazas a una entidad remota, por ejemplo, un sistema u operador que podría ser capaz de reducir la intrusión y/o amenaza.

Algunos ejemplos de la divulgación incluyen un sistema para monitorizar, detectar y/o reducir las amenazas de seguridad a los dispositivos de IoT utilizando la información de telemetría sobre el estado de seguridad del dispositivo de IoT, utilizando los datos de telemetría y utilizando otros datos del entorno de otros dispositivos de IoT. En algunos ejemplos, los agentes de recopilación de datos se implementan en dispositivos de IoT, y los datos sensoriales generados por tales dispositivos de IoT se utilizan para modelar y detectar las amenazas de seguridad para los dispositivos de IoT. Estos agentes de recopilación de datos pueden configurarse de forma remota utilizando los datos de configuración.

En algunos ejemplos, pueden utilizarse múltiples agentes en varios dispositivos de IoT para recopilar diversos tipos de datos que después pueden utilizarse en conjunto para formar un modelo más integral de operación e intrusión del dispositivo. En algunos ejemplos, los datos del agente del propio dispositivo de IoT se utilizan para informar el estado de seguridad del dispositivo de IoT. En algunos

ejemplos, los datos del agente de un conjunto de dispositivos se utilizan para formar un modelo del entorno operativo. En algunos ejemplos, se utilizan los datos de telemetría de múltiples dispositivos de IoT en el entorno y se forma un modelo del entorno.

En algunos ejemplos, el modelo resultante se utiliza para detectar las amenazas de seguridad como intrusiones y/o manipulación.

Dispositivos ilustrativos/entornos operativos

La figura 1 es un diagrama del entorno 100 en el cual pueden ponerse en práctica los aspectos de la tecnología. Tal como se muestra, el entorno 100 incluye los dispositivos informáticos 110, así como nodos de red 120, conectados a través de la red 130. Aunque en la figura 1 se muestran componentes particulares del entorno 100, en otros ejemplos, el entorno 100 también puede incluir componentes adicionales y/o diferentes. Por ejemplo, en ciertos ejemplos, el entorno 100 también puede incluir dispositivos de almacenamiento en red, administradores de mantenimiento y/u otros componentes adecuados (no mostrados). Los dispositivos informáticos 110 mostrados en la figura 1 pueden encontrarse en varios lugares, incluso en las instalaciones, en la nube o similares. Por ejemplo, los dispositivos informáticos 110 pueden encontrarse en el cliente, en el servidor, o similares.

Tal como se muestra en la figura 1, la red 130 puede incluir uno o más nodos de red 120 que interconectan múltiples dispositivos informáticos 110, y conectan los dispositivos informáticos 110 a la red externa 140, por ejemplo, internet o una intranet. Por ejemplo, los nodos de red 120 pueden incluir conmutadores, encaminadores, concentradores, controladores de red u otros elementos de red. En ciertos ejemplos, los dispositivos informáticos 110 pueden organizarse en bastidores, zonas de acción, grupos, conjuntos u otras divisiones adecuadas. Por ejemplo, en el ejemplo ilustrado, los dispositivos informáticos 1 a 10 se agrupan en tres conjuntos de computadoras centrales identificados individualmente como primero, segundo y tercer conjunto de computadoras centrales 112a-112c. En el ejemplo ilustrado, cada uno de los conjuntos de computadoras centrales 112a-112c está conectado operativamente a un nodo de red correspondiente 120a-120c, respectivamente, a los cuales comúnmente se les denomina nodos de red ubicados en la “parte superior del bastidor” (TOR, por sus siglas en inglés). Los nodos de red TOR 120a-120c pueden conectarse operativamente a los nodos de red 120 adicionales para formar una red informática en una topología jerárquica, plana, reticular u otro tipo adecuado que permita las comunicaciones entre los dispositivos informáticos 110 y la red externa 140. En otros ejemplos, los múltiples conjuntos de computadoras centrales 112a-112c pueden compartir un solo nodo de red 120. Los dispositivos informáticos 110 pueden ser virtualmente cualquier tipo de dispositivo informático de uso general o específico. Por ejemplo, estos dispositivos informáticos pueden ser dispositivos de usuario como computadoras de escritorio, computadoras portátiles, tabletas, dispositivos de presentación, cámaras, impresoras o teléfonos inteligentes. Sin embargo, en un entorno de centro de datos, estos dispositivos informáticos pueden ser dispositivos servidor como computadoras servidor de aplicaciones, computadoras centrales de computación virtual o computadoras servidor de archivos. Además, los dispositivos informáticos 110 pueden configurarse individualmente para proporcionar

servicios informáticos, de almacenamiento y/u otros servicios informáticos adecuados.

En algunos ejemplos, uno o más de los dispositivos informáticos 110 son un dispositivo de IoT, dispositivo de puerta de enlace, dispositivo que comprende parte o totalidad de un concentrador de IoT, dispositivo que comprende parte o totalidad de un servicio de portal de dispositivos, o similares, tal como se explica con mayor detalle posteriormente.

Dispositivo informático ilustrativo

La figura 2 es un diagrama que ilustra un ejemplo de dispositivo informático 200 en el cual pueden ponerse en práctica los aspectos de la tecnología. El dispositivo informático 200 puede ser prácticamente cualquier tipo de dispositivo informático de uso general o específico. Por ejemplo, el dispositivo informático 200 puede ser un dispositivo de usuario como una computadora de escritorio, computadora portátil, tableta, dispositivo de presentación, cámara, impresora o teléfono inteligente. Del mismo modo, el dispositivo informático 200 también puede ser un dispositivo servidor, como una computadora servidor de aplicaciones, computadora central de computación virtual, o una computadora servidor de archivos, por ejemplo, el dispositivo informático 200 puede ser un ejemplo del dispositivo informático 110 o nodo de red 120 de la figura 1. El dispositivo informático 200 también puede ser un dispositivo de IoT que se conecta a una red para recibir los servicios de IoT. Del mismo modo, el dispositivo informático 200 puede ser un ejemplo de cualquiera de los dispositivos ilustrados o representados en las figuras 3-5, tal como se explica con mayor detalle posteriormente. Tal como se ilustra en la figura 2, el dispositivo informático 200 incluye el circuito de procesamiento 210, memoria de operación 220, controlador de memoria 230, memoria de almacenamiento de datos 250, interfaz de entrada 260, interfaz de salida 270 y adaptador de red 280. Cada uno de estos componentes del dispositivo informático 200 enumerados anteriormente incluye al menos un elemento de *hardware*.

El dispositivo informático 200 incluye al menos un circuito de procesamiento 210 configurado para ejecutar las instrucciones, como instrucciones para implementar las cargas de trabajo, procesos o tecnología descritos en el presente documento. El circuito de procesamiento 210 puede incluir un microprocesador, microcontrolador, procesador gráfico, coprocesador, matriz de puertas programable *in-situ*, dispositivo lógico programable, procesador de señales o cualquier otro circuito adecuado para procesar datos. Las instrucciones anteriormente mencionadas, junto con otros datos (por ejemplo, conjuntos de datos, metadatos, instrucciones del sistema operativo, etcétera), pueden almacenarse en la memoria operativa 220 durante el tiempo de ejecución del dispositivo informático 200. La memoria operativa 220 también puede incluir cualquiera de una variedad de dispositivos/componentes de almacenamiento de datos, como memorias volátiles, memorias semivolátiles, memorias de acceso aleatorio, memorias estáticas, memorias caché, memorias tampón u otros medios utilizados para almacenar información en tiempo de ejecución. En un ejemplo, la memoria operativa 220 no retiene información cuando el dispositivo informático 200 está apagado. Más bien, el dispositivo informático 200 puede configurarse para transferir las instrucciones desde un componente de almacenamiento de datos no volátil (por ejemplo, el componente de almacenamiento de datos 250) a la memoria operativa 220

como parte de un proceso de arranque u otro proceso de carga.

La memoria operativa 220 puede incluir memoria de tasa de datos doble de cuarta generación (DDR4, por sus siglas en inglés), memoria de tasa de datos doble de tercera generación (DDR3, por sus siglas en inglés), otra memoria de acceso aleatorio dinámico (DRAM, por sus siglas en inglés), memoria de alto ancho de banda (HBM, por sus siglas en inglés), memoria cubo de memoria híbrida, memoria apilada tridimensional, memoria estática de acceso aleatorio (SRAM, por sus siglas en inglés) u otra memoria, y tal memoria puede comprender uno o más circuitos de memoria integrados en un DIMM, SIMM, SODIMM u otro paquete. Tales módulos o dispositivos de memoria operativa pueden organizarse de acuerdo con canales, rangos y bancos. Por ejemplo, los dispositivos de memoria operativa pueden conectarse al circuito de procesamiento 210 a través del controlador de memoria 230 en canales. Un ejemplo de dispositivo informático 200 puede incluir uno o dos módulos DIMM por canal, con uno o dos rangos por canal. La memoria operativa dentro de un rango puede operar con un reloj compartido, y una dirección compartida y un bus de comando. Además, un dispositivo de memoria operativa puede organizarse en varios bancos en los cuales puede considerarse a un banco como una matriz direccionada por fila y columna. De acuerdo con una organización de memoria operativa de este tipo, las direcciones físicas dentro de la memoria operativa pueden consultarse por un conjunto de variables de canal, rango, banco, fila y columna.

A pesar del análisis anterior, la memoria operativa 220 específicamente no incluye ni abarca medios de comunicación, ningún soporte de comunicación ni ninguna señal *per se*.

El controlador de memoria 230 está configurado para interconectar el circuito de procesamiento 210 a la memoria operativa 220. Por ejemplo, el controlador de memoria 230 puede configurarse para interconectar comandos, direcciones y datos entre la memoria operativa 220 y el circuito de procesamiento 210. El controlador de memoria 230 también puede estar configurado para compendiar o gestionar de otro modo ciertos aspectos de la gestión de la memoria desde o para el circuito de procesamiento 210. Aunque el controlador de memoria 230 se ilustra como un controlador de memoria único separado del circuito de procesamiento 210, en otros ejemplos, pueden emplearse múltiples controladores de memoria, los controladores de memoria pueden integrarse con la memoria operativa 220, o similar. Además, los controladores de memoria pueden integrarse en el circuito de procesamiento 210. Estas y otras variaciones son posibles.

En el dispositivo informático 200, la memoria de almacenamiento de datos 250, interfaz de entrada 260, interfaz de salida 270 y adaptador de red 280 están interconectados al circuito de procesamiento 210 por el bus 240. Aunque, la figura 2 ilustra el bus 240 como un bus pasivo único, otras configuraciones, como un conjunto de buses, conjunto de enlaces de punto a punto, controlador de entrada/salida, puente, otros circuitos de interconexión o cualquier conjunto de los mismos también pueden emplearse adecuadamente para interconectar la memoria de almacenamiento de datos 250, interfaz de entrada 260, interfaz de salida 270 o adaptador de red 280 al circuito de procesamiento 210.

En el dispositivo informático 200, la memoria de almacenamiento de datos 250 se emplea para el almacenamiento de datos no volátil a largo plazo. La memoria de almacenamiento de datos 250 puede

incluir cualquiera de una variedad de dispositivos/componentes de almacenamiento de datos no volátiles, como memorias no volátiles, discos, unidades de disco, unidades de disco duro, unidades de estado sólido o cualquier otro medio que pueda utilizarse para el almacenamiento no volátil de la información. Sin embargo, la memoria de almacenamiento de datos 250 específicamente no incluye ni abarca medios de comunicación, ningún soporte de comunicación ni ninguna señal *per se*. A diferencia de la memoria operativa 220, la memoria de almacenamiento de datos 250 se emplea por el dispositivo informático 200 para el almacenamiento no volátil de datos a largo plazo, en lugar de para el almacenamiento de datos en tiempo de ejecución.

Además, el dispositivo informático 200 puede incluir o estar conectado a cualquier tipo de medios legibles por el procesador, como medios de almacenamiento legibles por el procesador (por ejemplo, memoria operativa 220 y memoria de almacenamiento de datos 250) y medios de comunicación (por ejemplo, señales de comunicación y ondas de radio). Aunque el término medio de almacenamiento legible por el procesador incluye la memoria operativa 220 y la memoria de almacenamiento de datos 250, el término “medio de almacenamiento legible por el procesador”, a lo largo de la especificación y reivindicaciones, ya sea que se utilice en singular o en plural, se define en el presente documento, de modo que el término “medio de almacenamiento legible por el procesador” excluya específicamente y no abarque los medios de comunicación, ningún soporte de comunicación ni señal *per se*. Sin embargo, el término “medio de almacenamiento legible por el procesador” abarca la memoria caché del procesador, memoria de acceso aleatorio (RAM, por sus siglas en inglés), memoria de registro y/o similares.

El dispositivo informático 200 también incluye una interfaz de entrada 260, que puede configurarse para permitir que el dispositivo informático 200 reciba información de parte de los usuarios o de otros dispositivos. Además, el dispositivo informático 200 incluye la interfaz de salida 270, que puede configurarse para proporcionar la salida del dispositivo informático 200. En un ejemplo, la interfaz de salida 270 incluye una memoria tampón de fotogramas, procesador de gráficos, procesador o acelerador de gráficos, y está configurado para representar presentaciones para que se muestren en un dispositivo de presentación visual separado (como un monitor, proyector, computadora cliente de computación virtual, etcétera). En otro ejemplo, la interfaz de salida 270 incluye un dispositivo de presentación visual y está configurada para representar y mostrar las porciones para la visualización.

En el ejemplo ilustrado, el dispositivo informático 200 está configurado para comunicarse con otros dispositivos informáticos o entidades a través del adaptador de red 280. El adaptador de red 280 puede incluir un adaptador de red alámbrico, por ejemplo, un adaptador Ethernet, adaptador de anillo de testigo o un adaptador digital o adaptador de línea de suscriptor (DSL, por sus siglas en inglés). El adaptador de red 280 también puede incluir un adaptador de red inalámbrica, por ejemplo, un adaptador de wifi, adaptador de Bluetooth, adaptador de ZigBee, adaptador de evolución a largo plazo (LTE, por sus siglas en inglés) o un adaptador de 5G.

Aunque el dispositivo informático 200 se ilustra con ciertos componentes configurados en una disposición particular, estos componentes y la disposición son simplemente un ejemplo de un dispositivo informático en el cual puede emplearse la tecnología. En otros ejemplos, la memoria de almacenamiento

de datos 250, interfaz de entrada 260, interfaz de salida 270 o adaptador de red 280 pueden conectarse directamente al circuito de procesamiento 210 o circuito de procesamiento 210 a través de un controlador de entrada/salida, puente u otro circuito de interconexión. Otras variaciones de la tecnología son posibles.

Algunos ejemplos del dispositivo informático 200 incluyen al menos una memoria (por ejemplo, memoria operativa 220) adaptada para almacenar datos en tiempo de ejecución y al menos un procesador (por ejemplo, unidad de procesamiento 210) que están adaptados respectivamente para ejecutar código ejecutable por procesador que, en respuesta a la ejecución, permite que el dispositivo informático 200 realice acciones. En algunos ejemplos, el dispositivo informático 200 está habilitado para realizar acciones como las acciones en el proceso de las posteriores figuras 4 o 5, o acciones en un proceso realizado por uno o más de los dispositivos informáticos en la posterior figura 3.

Sistema ilustrativo

La figura 3 es un diagrama de bloques que ilustra un ejemplo de un sistema (300) para comunicaciones de IoT. El sistema 300 puede incluir la red 330, concentrador de IoT 351, dispositivos de IoT 341-343, dispositivos de puerta de enlace 311 y 312 y servicio de portal de dispositivos 313, todos ellos se conectan a la red 330. Tal como se explicó anteriormente, el término “concentrador de IoT” no se limita a un tipo particular de servicio de IoT, pero se refiere al dispositivo con el cual se comunica el dispositivo de IoT, después del aprovisionamiento, para al menos una solución de IoT o un servicio de IoT de cualquier tipo. Es decir, el término “concentrador de IoT”, tal como se utiliza en toda la especificación y reivindicaciones, es genérico para cualquier solución de IoT. El término “dispositivo de IoT” se refiere a un dispositivo que utiliza o está destinado a hacer uso de los servicios de IoT. Un dispositivo de IoT puede incluir prácticamente cualquier dispositivo que se conecte a la nube para utilizar los servicios de IoT, incluso para la recopilación de telemetría o cualquier otro propósito. El servicio de portal de dispositivos 313 incluye uno o más dispositivos que proporcionan un portal de dispositivos. El término “concentrador de IoT” se refiere a un dispositivo, o varios dispositivos, como un sistema distribuido, al cual los dispositivos de IoT se conectan a través de la red para los servicios de IoT.

Cada uno de los dispositivos de IoT 341-343, dispositivos de puerta de enlace 311 y 312, y/o dispositivos que comprenden el concentrador de IoT 351 y/o el servicio de portal de dispositivos 313 pueden incluir ejemplos del dispositivo de computación 200 de la figura 2. La figura 3 y la descripción correspondiente de la figura 3 en la especificación ilustran un sistema ejemplar con fines ilustrativos que no limita el alcance de la divulgación.

La red 330 puede incluir una o más redes informáticas, que incluyen redes alámbricas y/o inalámbricas, donde cada red puede ser, por ejemplo, una red inalámbrica, red de área local (LAN, por sus siglas en inglés), red de área amplia (WAN, por sus siglas en inglés), y/o red global como internet. En un conjunto interconectado de LAN, que incluye aquellas basadas en diferentes arquitecturas y protocolos, un encaminador actúa como un enlace entre las LAN, permitiendo que los mensajes se envíen entre ellas. Además, los enlaces de comunicación dentro de las LAN comúnmente incluyen un par de cables trenzados o un cable coaxial, mientras los enlaces de comunicación entre redes pueden utilizar

líneas telefónicas analógicas, líneas digitales dedicadas completas o fraccionadas que incluyen T1, T2, T3 y T4, redes digitales de servicios integrados (RDSI, por sus siglas en inglés), líneas de suscriptor digital (DSL, por sus siglas en inglés), enlaces inalámbricos que incluyen enlaces satelitales u otros enlaces de comunicaciones conocidos para los expertos en la técnica. Además, las computadoras remotas y otros dispositivos electrónicos relacionados podrían conectarse de forma remota a las redes LAN o WAN a través de un módem y un enlace telefónico temporal. En esencia, la red 330 incluye cualquier método de comunicación mediante el cual la información puede transmitirse entre el concentrador de IoT 351, dispositivos de IoT 341-343, dispositivos de puerta de enlace 311-312 y servicio de portal de dispositivos 313.

Como un ejemplo, los dispositivos de IoT 341-343 son dispositivos que están destinados a hacer uso de los servicios de IoT proporcionados por uno o más concentradores de IoT, como el concentrador de IoT 351. El servicio de portal de dispositivos 313 incluye un dispositivo o varios dispositivos que realizan acciones en el suministro de un portal de dispositivos para los usuarios de los dispositivos de IoT.

Los dispositivos de puerta de enlace opcionales 311 y 312 son dispositivos que algunos dispositivos de IoT 341-343 pueden utilizar para acceder al concentrador de IoT 351. En algunos ejemplos, después del aprovisionamiento, algunos o todos los dispositivos de IoT 341-343 se comunican con el concentrador de IoT 351 sin utilizar un intermediario. En otros ejemplos, algunos o todos los dispositivos de IoT 341-343 se comunican con el concentrador de IoT 351 utilizando un dispositivo intermediario como uno o más de los dispositivos de puerta de enlace 311 y 312. El servicio de portal de dispositivos 313 es un servicio que pueden utilizar los usuarios de los dispositivos de IoT para gestionar los servicios de IoT para los dispositivos de IoT, que incluyen los dispositivos de IoT 341-343.

El sistema 300 puede incluir más o menos dispositivos que los ilustrados en la figura 3, que se muestran a modo de ejemplo solamente.

Procesos ilustrativos

Para mayor claridad, los procesos descritos en el presente documento se describen en términos de operaciones realizadas en secuencias particulares por dispositivos o componentes particulares de un sistema.

Sin embargo, se observa que otros procesos no se limitan a las secuencias, dispositivos o componentes establecidos. Por ejemplo, ciertas acciones pueden realizarse en diferentes secuencias, simultáneamente, omitirse, o pueden complementarse con acciones o características adicionales, ya sea que tales secuencias, paralelismos, acciones o características se describan o no en el presente documento. Del mismo modo, cualquier tecnología descrita en la presente divulgación puede incorporarse en los procesos descritos u otros procesos, ya sea que esa tecnología se describa específicamente o no en conjunto con un proceso. Los procesos descritos también pueden realizarse en o por otros dispositivos, componentes o sistemas, ya sea que tales dispositivos, componentes o sistemas se describan o no en el presente documento. Estos procesos también pueden materializarse de varias

maneras. Por ejemplo, pueden incorporarse a un producto manufacturado, por ejemplo, como instrucciones legibles por el procesador almacenadas en un medio de almacenamiento legible por el procesador o realizarse como un proceso implementado por computadora. Como un ejemplo alternativo, estos procesos pueden codificarse como instrucciones ejecutables por el procesador y transmitirse a través de un medio de comunicación.

La figura 4 es un diagrama que ilustra un flujo de datos ejemplar para un proceso (420) para la autenticación de IoT. La figura 4 y la descripción correspondiente de la figura 4 en la especificación ilustran un proceso ejemplar para fines ilustrativos que no limita el alcance de la divulgación.

En el ejemplo ilustrado, primero, se produce la etapa 421. En la etapa 421, el concentrador de IoT 451 almacena un conjunto de reglas de seguridad asociadas con una condición esperada de al menos un dispositivo de IoT (por ejemplo, el dispositivo de IoT 441). En algunos ejemplos, el conjunto de reglas de seguridad se basa en una evaluación de los datos de IoT asociados con al menos un dispositivo de IoT (por ejemplo, dispositivo de IoT 441). El conjunto de reglas de seguridad almacenadas puede ser diferente, por ejemplo, con base en el tipo de dispositivo de IoT, en el contexto de implementación particular y otros factores. El conjunto de reglas de seguridad se analiza con mayor detalle posteriormente (después del análisis de los datos de IoT recopilados en la posterior etapa 424).

Tal como se muestra, la etapa 422 se produce a continuación en algunos ejemplos. En la etapa 422, una solicitud de configuración puede generarse por el servicio de portal de dispositivos 413 y después la solicitud de configuración puede comunicarse desde el servicio de portal de dispositivos 413 al concentrador de IoT 451. La solicitud de configuración puede estar asociada con el ajuste del conjunto de reglas de seguridad almacenadas en el concentrador de IoT 451. En algunos ejemplos, la solicitud de configuración es una solicitud para cambiar un conjunto de reglas de seguridad a un conjunto ajustado de reglas de seguridad. La solicitud de configuración puede realizarse de diferentes maneras en diferentes ejemplos. En algunos ejemplos, existe un modo básico en el cual se utiliza el conjunto predeterminado de reglas de seguridad, y también existe una configuración avanzada donde el usuario puede realizar una solicitud de configuración para cambiar el conjunto predeterminado de reglas de seguridad. Tal como se muestra, la etapa 423 se produce a continuación en algunos ejemplos. En la etapa 423, el concentrador de IoT 451 puede ajustar el conjunto de reglas de seguridad almacenadas en el concentrador de IoT 451 con base en la solicitud de configuración recibida desde el servicio de portal de dispositivos 413 en la etapa 422.

Tal como se muestra, la etapa 424 se produce a continuación en algunos ejemplos. En la etapa 424, el dispositivo de IoT 441 recibe y recopila los datos de entorno a partir del entorno, por ejemplo, el entorno cercano al dispositivo de IoT 441, y recopila los datos sobre el estado de seguridad interno del dispositivo de IoT 441. Los datos de entorno pueden incluir datos de telemetría, datos que indican si el dispositivo de IoT 441 se manipuló físicamente o no. Los datos de telemetría pueden incluir temperatura, humedad, ocupación de una ubicación asociada con el dispositivo de IoT, geolocalización y/o similares. Los datos sobre el estado de seguridad interna del dispositivo de IoT 441 pueden incluir la versión del sistema operativo (OS, por sus siglas en inglés), estado actual de los procesos activos, puertos abiertos,

direcciones de protocolo de internet (IP, por sus siglas en inglés) de los dispositivos conectados y/o similares. Los datos pueden recopilarse mediante entradas de *software*, entradas de *hardware* o ambas.

Los datos de telemetría recopilados en la etapa 424 pueden incluir telemetría que el dispositivo de IoT ya recopiló en algunos ejemplos. Por ejemplo, un dispositivo de IoT que es un sensor de temperatura ya puede estar configurado para recopilar los datos de temperatura.

El dispositivo de IoT 441 puede tener uno o más interruptores de manipulación que detectan la manipulación física. En un ejemplo, el interruptor de manipulación se desactiva si el dispositivo de IoT 441 no se manipuló físicamente, y el interruptor de manipulación se activa si el dispositivo de IoT 441 se manipuló físicamente. Los datos de entorno pueden incluir una indicación de si el interruptor de manipulación está activado o desactivado. Por ejemplo, en algunos ejemplos, el dispositivo de IoT 441 tiene una cubierta que está conectada a dos interruptores de manipulación. Si se abre la cubierta, ambos interruptores de manipulación se activan.

En algunos ejemplos, el dispositivo de IoT 441 puede incluir un agente de *software* que recopila los datos de entorno y los datos sobre la seguridad interna del dispositivo de IoT 441. En algunos ejemplos, el dispositivo de IoT 441 tiene un agente de *software* de recopilación de datos implementado en el dispositivo de IoT 441 para recopilar los datos de entorno y/o del estado interno. En algunos ejemplos, algunos o todos los dispositivos de IoT tienen un agente de *software* de recopilación de datos implementado en el dispositivo de IoT para recopilar los datos de entorno y/o del estado interno de los dispositivos de IoT.

El conjunto de reglas de seguridad almacenadas en el concentrador de IoT 451 se basa en un modelo del comportamiento normal de los dispositivos de IoT (por ejemplo, 441 y/o 341-434 de la figura 3). Este modelo puede representar el estado de los dispositivos de IoT mientras estos dispositivos funcionan en condiciones normales. En algunos ejemplos, el conjunto de reglas de seguridad actúa como un modelo configurable de dispositivo de IoT. El conjunto de reglas puede definirse de tal manera que se infrinja el conjunto de reglas si se produce un ataque u otra intrusión de seguridad o amenaza de seguridad.

Por ejemplo, los dispositivos de IoT pueden estar sujetos a varios tipos de ataques de seguridad que pueden clasificarse en dos categorías: ataques cibernéticos y ataques físicos. Los ataques cibernéticos incluyen ataques a las propiedades cibernéticas de los dispositivos, como en el sistema operativo, infraestructura de red, conexión y datos. Los ataques físicos incluyen ataques como manipulación física de los dispositivos, manipulación de los elementos de generación de datos de los dispositivos, reubicación y similares. En algunos ejemplos, el conjunto de reglas de seguridad se genera o ajusta de tal manera que la infracción del conjunto de reglas de seguridad indique al menos una posibilidad de un ataque (por ejemplo, un ataque físico o un ciberataque) en uno o más dispositivos de IoT. En consecuencia, una vez que ocurra cualquiera de estos ataques, debe producirse una infracción del conjunto de reglas en un ejemplo, puesto que los datos recopilados a partir de los dispositivos serán contrarios al modelo. El modelo puede incluir uno o más patrones para los datos de telemetría.

En consecuencia, el conjunto de reglas de seguridad puede definir las condiciones de operación

normal que, si no se cumplen, pueden indicar la posibilidad de una amenaza para la seguridad. Por ejemplo, el conjunto de reglas de seguridad puede infringirse si uno o más de los elementos de datos están fuera de un rango esperado. Por ejemplo, el conjunto de reglas de seguridad puede requerir que la temperatura esté en un cierto rango, que el interruptor de manipulación esté desactivado, que ciertos procesos de la lista negra no se estén ejecutando y/o similares. Los rangos esperados o los valores discretos esperados pueden depender de la hora del día y de otros factores. En algunos ejemplos, en lugar de simplemente comparar cada tipo de datos, como la temperatura o similar, con un rango esperado (o valor discreto esperado) individualmente, el conjunto de reglas de seguridad se basa en varios tipos de datos considerados en conjunto, con base en un modelo. Por ejemplo, en algunos ejemplos, la temperatura en el entorno por encima del rango esperado puede no resultar en una infracción de las reglas de seguridad a menos que también exista ocupación en el entorno.

En algunos ejemplos, el conjunto de reglas de seguridad se basa en un modelo de los datos de seguridad interna y de entorno recopilados por los dispositivos de IoT, donde el modelo proporciona efectivamente una representación “única” de los datos esperados. La representación única puede reflejar el comportamiento normal de los dispositivos de IoT en condiciones de funcionamiento normal sin ninguna intrusión o amenaza de seguridad. Si, con base en los datos de IoT recibidos, algunos aspectos difieren de la representación única, el conjunto de reglas puede considerarse infringido de acuerdo con otros datos. Por ejemplo, de acuerdo con la representación única de un sensor de ocupación de una habitación en particular en el centro comercial, el sensor de ocupación no debe mostrar la ocupación durante ciertas horas en las cuales no se espera que nadie esté presente en el centro comercial. Sin embargo, las reglas pueden especificar que, por ejemplo, si la puerta del centro comercial está abierta y el guardia todavía está presente en el centro comercial, la ocupación en el momento inesperado no activa una infracción del conjunto de reglas de seguridad. En algunos ejemplos, los datos de múltiples dispositivos de IoT pueden estar involucrados en el modelo y el conjunto de reglas de seguridad para determinar si el conjunto de reglas se ha infringido o no. Al utilizar los datos de múltiples dispositivos de IoT, puede utilizarse un modelo más integral de la operación de dispositivo y del entorno de operación y de intrusión en comparación de si el modelo estuviera basado en un dispositivo de IoT.

En algunos ejemplos, el conjunto de reglas de seguridad incluye una o ambas de una lista blanca de procesos y una lista negra de procesos. La lista blanca y la lista negra de procesos pueden ser útiles para determinar si un dispositivo de IoT se ha sido infectado por un programa malicioso o no. Una “lista blanca” de proceso se refiere a una lista de procesos aprobados, y una “lista negra” de procesos se refiere a una lista de procesos prohibidos.

En algunos ejemplos, los datos de IoT recopilados, que incluyen los datos de telemetría recopilados, pueden utilizarse para ayudar a construir el modelo para crear o ajustar el conjunto de reglas de seguridad.

Tal como se muestra, la etapa 425 se produce a continuación en algunos ejemplos. En la etapa 425, el dispositivo de IoT 441 puede determinar si enviar o no los datos al concentrador de IoT 451. En algunos ejemplos, en la etapa 425, el dispositivo de IoT 441 simplemente determina enviar siempre todos

los datos al concentrador de IoT 451. En algunos ejemplos, los datos solo se envían después de superar un umbral con base en uno o más de los tipos de datos.

Por ejemplo, en algunos ejemplos, el dispositivo de IoT 441 determina enviar los datos de temperatura solo si la temperatura detectada está fuera de un rango predeterminado, tal como 18.33-23.89°C (65-75°F). En algunos ejemplos, el hecho de que la temperatura esté fuera del intervalo de 18.33-23.89°C (65-75°F) no constituye en sí una infracción de las reglas de seguridad. El dispositivo de IoT 441 no determina si o no el conjunto de reglas de seguridad se infringió, en este ejemplo, pero solo envía los datos de temperatura cuando la temperatura está fuera de un intervalo particular, y, por lo tanto, podría existir una infracción del conjunto de reglas de seguridad dependiendo de otros factores.

Tal como se muestra, la etapa 426 ocurre a continuación en algunos ejemplos cuando la determinación en la etapa 425 es positiva. En la etapa 426, los datos de IoT pueden comunicarse desde el dispositivo de IoT 441 al concentrador de IoT 451. Si, por el contrario, la determinación en la etapa 426 es negativa, se reanuda el procesamiento.

Tal como se muestra, en algunos ejemplos, la etapa 427 se produce a continuación después de la etapa 426. En la etapa 427, el concentrador de IoT 451 determina, con base en los datos de IoT recibidos en la etapa 426, en cuanto a si se infringió el conjunto de reglas de seguridad almacenado en el concentrador de IoT 451. En algunos ejemplos, la determinación en la etapa 427 es una comparación de los datos agregados del dispositivo de IoT con el modelo configurable del dispositivo de IoT.

Tal como se muestra, la etapa 428 se produce a continuación en algunos ejemplos. En la etapa 428, el concentrador de IoT 451 envía selectivamente una alerta al servicio de portal de dispositivos 413 con base en la determinación de la etapa 427. Si en la etapa 427 se determinó que se infringieron las reglas, el concentrador de IoT 451 comunica una alerta al servicio de portal de dispositivos 413 si, en cambio, en la etapa 427 se determinó que el conjunto de reglas no se infringió, el concentrador de IoT 451 no envía una alerta.

Si el dispositivo de IoT 441 se desconecta de la nube, los datos no pueden recopilarse desde el dispositivo de IoT 441, pero el hecho de que el dispositivo de IoT 441 se desconecte de la nube es en sí mismo una forma de información y, en algunos ejemplos, puede surgir una alerta en cuanto a que el dispositivo de IoT 441 se desconecta de la nube.

En algunos ejemplos, el conjunto de reglas de seguridad puede ajustarse aún más durante el transcurso del tiempo, tanto para reducir los falsos positivos como para detectar con éxito los ataques que de otro modo no podrían detectarse. En algunos ejemplos, el concentrado de IoT 451 incluye una capa de aprendizaje que aprende a partir de las anomalías y se adapta al cambiar el conjunto de reglas de seguridad durante el transcurso del tiempo y al aprender durante el transcurso del tiempo.

En algunos ejemplos, en lugar de enviar los datos de IoT directamente al concentrador de IoT 451, el dispositivo de IoT 441 envía los datos a un dispositivo de puerta de enlace (por ejemplo, el dispositivo de puerta de enlace 311 o 312 de la figura 3). En algunos ejemplos, el dispositivo de puerta de enlace, en lugar del dispositivo de IoT 440, determina si enviar o no los datos de IoT al concentrador de IoT 451. En algunos ejemplos, existen varios dispositivos de IoT diferentes (por ejemplo, 341-343 de la

figura 3) envían los datos de IoT a un dispositivo de puerta de enlace, que agrega los datos antes de determinar si y qué datos de IoT se enviarán al concentrador de IoT 451.

En algunos ejemplos, en la etapa 428, en lugar de simplemente enviar una alerta, otros detalles, que incluyen, por ejemplo, la información sobre el tipo del ataque o amenaza, hasta donde pueda determinarse, también se comunican desde el concentrador de IoT 451 al servicio de portal de dispositivos 413 junto con la alerta. Por ejemplo, si el concentrador de IoT 451 determina a través de GPS que un dispositivo se movió y a partir de otros datos de IoT que un programa malicioso se instaló, entonces la naturaleza de este ataque puede comunicarse desde el concentrador de IoT 451 al servicio de portal de dispositivos 413, que es potencialmente un caso diferente que si solo uno de estos dos eventos hubiera ocurrido. Los datos agregados a partir de múltiples dispositivos de IoT también pueden utilizarse, cuando corresponda, para describir con más detalle el tipo de la amenaza a la seguridad en una comunicación desde el concentrador de IoT 451 al servicio de portal de dispositivos 413.

La figura 5 es un diagrama de flujo lógico que ilustra un ejemplo de un proceso (590) para la autenticación de IoT. En un ejemplo, el proceso 590 se realiza mediante un concentrador de IoT, como el concentrador de IoT 351 de la figura 1. Después de un bloque de inicio, el proceso procede al bloque 591. En el bloque 591, se almacena un conjunto de reglas de seguridad asociadas con una condición esperada de al menos un dispositivo de IoT. El proceso entonces procede al bloque 592. En el bloque 592, se reciben los datos de IoT asociados con al menos un dispositivo de IoT. Los datos de IoT pueden ser datos agregados que incluyen al menos dos tipos diferentes de datos. El proceso entonces procede al bloque de decisión 593.

En el bloque de decisión 593, se realiza una determinación, con base en los datos de IoT, en cuanto a si se ha infringido el conjunto de reglas de seguridad. Si la determinación en el bloque de decisión 593 es negativa, el proceso procede a un bloque de retorno, donde se reanuda otro procesamiento. Si, en cambio, la determinación en el bloque de decisión 593 es positiva, el proceso procede al bloque 594, donde se envía una alerta. Por ejemplo, en algunos ejemplos, la alerta se envía a un servicio de portal de dispositivos. Entonces, el proceso procede a un bloque de retorno, donde se reanuda el procesamiento. De esta manera, se envía una alerta de forma selectiva con base en la determinación en el bloque de decisión 593.

Conclusión

Aunque la descripción detallada anterior describe ciertos ejemplos de la tecnología y describe el mejor modo contemplado, sin importar qué tan detallado aparezca lo anterior en el texto, la tecnología puede ponerse en práctica de muchas maneras. Los detalles pueden variar en la implementación, aunque aún están abarcados por la tecnología descrita en el presente documento. Tal como se indicó anteriormente, no debe considerarse que la terminología particular utilizada al describir ciertas características o aspectos de la tecnología implica que la terminología se está redefiniendo en el presente documento para restringirla a cualquier característica, propiedad o aspecto específicos con los cuales se asocia esa terminología. En general, los términos utilizados en las siguientes reivindicaciones no deben

interpretarse como limitantes de la tecnología a los ejemplos específicos descritos en el presente documento, a menos que la descripción detallada defina explícitamente tales términos. En consecuencia, el alcance real de la tecnología abarca no solo los ejemplos divulgados, sino también todas las formas equivalentes de poner en práctica o implementar la tecnología.

5

10

15

20

25

30

35