

Señores

Superintendencia de Industria y Comercio

Dirección de Nuevas Creaciones

E. S. D.

Ref: Expediente No. NC2019/0004599.

Solicitud de registro de Patente de Invención denominada “APARATO Y MÉTODOS PARA SERVICIO DE SEGURIDAD DEL INTERNET DE LAS COSAS”.

Fase nacional de la solicitud PCT/US2017/058926.

Solicitante: MICROSOFT TECHNOLOGY LICENSING, LLC.

Luz Helena Adarve, identificada como aparece al pie de mi firma, y obrando en mi condición de apoderada de **MICROSOFT TECHNOLOGY LICENSING, LLC**, solicitante de la patente en referencia, a continuación, doy respuesta al Oficio **No. 2615** del 28 de febrero de 2022.

1. Respecto a la Determinación del Estado de la Técnica y al Examen de Patentabilidad

En los numerales 3, 4 y 5 del oficio citado, ese Despacho concluye que las reivindicaciones de la presente solicitud de patente carecen de nivel inventivo frente a las enseñanzas de los documentos **WO2016140912** (D1) y **US20150163121** (D2).

1.1. Novedad y nivel inventivo

El nuevo capítulo reivindicatorio ahora presentado es novedoso de acuerdo con el análisis de patentabilidad presentado en el del oficio No. **2615** porque, de acuerdo a dicho análisis, ninguna de las anterioridades divulga completamente la materia

reclamada en la solicitud. Teniendo en cuenta que las reivindicaciones del nuevo capítulo reivindicatorio que ahora se presenta mantienen las mismas características que fueron estudiadas en dicho oficio, este nuevo capítulo reivindicatorio es novedoso al menos por dichas características reconocidas como novedosas por este Despacho.

Adicionalmente, aunque el Examinador haya citado los documentos D1 y D2 para objetar la altura inventiva de la presente invención, es posible afirmar que éstos no enseñan las características esenciales de la invención que ahora se presentan en el nuevo capítulo reivindicatorio enmendado.

Con el fin de superar las objeciones presentadas respecto al nivel inventivo de las reivindicaciones, **es deseo del solicitante presentar un nuevo capítulo reivindicatorio compuesto por 20 reivindicaciones**, que encuentran su debido sustento en las reivindicaciones y la descripción originalmente presentadas, sin que ello conlleve ampliación de la invención.

Primero se indica que las reivindicaciones 1, 13, y 17 se modificaron con el objetivo de que sea aún más clara su novedad y nivel inventivo donde ahora incluyen que la determinación de si se infringió el conjunto de reglas de seguridad “se basa en los datos IoT ya recibidos y ocurre a continuación después de recibir dichos datos IoT” lo que no está divulgado ni sugerido por los documentos D1 o D2.

Esta característica está soportada en la página 13 de la descripción de la presente solicitud y en su figura 4. Para una rápida referencia, dicha página 13 menciona lo siguiente:

“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”.

En el párrafo anterior, según la figura 4, la etapa 427 corresponde a la determinación de si se infringió el conjunto de reglas de seguridad y la etapa 426 al envío de los datos IoT desde el dispositivo IoT.

Esta característica distintiva tiene la ventaja técnica que hace posible hacer un segundo análisis más detallado (correspondiente a una segunda determinación) sin la necesidad de recolectar más datos lo que volvería más complejo el proceso para garantizar un nivel alto de seguridad para los dispositivos IoT de una manera más eficiente, al menos más eficiente que las invenciones de los documentos D1 y D2.

El documento D1 se relaciona con el análisis de comportamiento para automatizar el monitoreo del estado de los dispositivos de Internet de las cosas (IoT) de manera directa o indirecta. En particular, el comportamiento normal asociado con un dispositivo IoT en una red IoT local puede modelarse de manera que los comportamientos observados en el dispositivo IoT se puedan comparar con el comportamiento normal modelado para determinar si los comportamientos observados en el dispositivo IoT son normales o anómalos.

La invención del documento D1, cuando transmite los parámetros de comportamiento observados a un servicio al cliente, no realiza la determinación de la violación de las reglas de seguridad a continuación después de su recepción, es decir, no realiza dicha determinación inmediatamente después de su recepción. Por el contrario, el documento D1, en su párrafo [0130] sugiere que, cuando se envían los parámetros de comportamiento observado a un servicio al cliente, para el diagnóstico de un comportamiento anómalo se habilitan mensajes de entrada y salida **para recolectar información adicional**, lo cual es contrario a lo reclamado en la presente solicitud que determina la violación a las reglas de seguridad con la información ya recibida, sin recolectar información adicional.

Por su parte, el documento D2 no solventa la mencionada falencia del documento D1 en divulgar la determinación de la violación con información ya recibida e inmediatamente después de recibirla. Por el contrario, el documento D2 requiere de un aumento en la supervisión para recopilación de datos adicionales antes de tomar una determinación final sobre la existencia o no de actividad maliciosa (ver documento D2, párrafo [0233]).

Adicionalmente, nótese que la invención que se reclama en la presente solicitud, **a diferencia de lo divulgado en el documento D1, requiere de dos**

determinaciones una realizada en el dispositivo IoT y otra en el en el concentrador IoT correspondientes a las siguiente:

- determinar, en el dispositivo IoT, si ha excedido un umbral basado en uno o más de los tipos de datos para que el dispositivo IoT envíe los datos, que son recibido en el concentrador IoT, para permitir una segunda determinación; y
- determinar, en el concentrador IoT, con base en los datos de IoT y en el modelo de dispositivo de IoT, si se infringió el conjunto de reglas de seguridad (593) para el dispositivo IoT.

Estas dos determinaciones permiten que la invención que se reclama garantice un nivel alto de seguridad para los dispositivos IoT de una manera más eficiente (al menos más eficiente que la invención del documento D1), debido a que la primera determinación, que es menos exigente computacionalmente, es la que determina si se envían los datos al concentrador IoT para que, en dicho concentrador, se determine si se infringió el conjunto de reglas de seguridad, lo cual es más exigente computacionalmente que la primera determinación.

De acuerdo con lo dicho en el anterior párrafo, la invención que se reclama aumenta la eficiencia porque realiza siempre determinaciones de baja exigencia computacional en el dispositivo IoT y solo realiza envío de datos y posterior procesamiento para determinar una posible violación de seguridad cuando existe un indicio de ello correspondiente a que un valor a excedido un umbral.

En contraste, las invenciones de los documentos D1 y D2 son diferentes y no presentan este efecto mejorado

Aunque el análisis de patentabilidad del oficio No 2615 alega que el documento D1 divulga ambas determinaciones, en realidad no lo hace. Dicho análisis de patentabilidad indica que la primera determinación (la que se realiza en el dispositivo IoT) esta divulgada en el párrafo [0129] y [0130] del documento D1, y la segunda determinación (la que se realiza en el concentrador IoT) esta divulgada en los párrafos [0130] y [0121]. La detección de anomalías que se determinan en los párrafos [0129] y [0130] se refieren a una misma determinación y corresponde a una sola determinación, y, por lo tanto, no corresponden a dos determinaciones diferentes y mucho menos a dos determinaciones consecutivas como se requiere en la invención de la presente solicitud. Por su parte el párrafo

[0121] se refiere a la recolección registros (logs) provenientes de los dispositivos IoT observadores, pero no divulga propiamente la determinación.

A saber, el documento D1 describe los dos siguientes casos alternativos (es decir, dos realizaciones diferentes, separadas y que no se combinan entre ellas):

- Un primer caso donde los dispositivos de IoT transmiten todos los datos de IoT a un potente dispositivo analizador (que podría interpretarse como un concentrador IoT), que posteriormente realiza un análisis de comportamiento para determinar si los comportamientos observados en los dispositivos de IoT son normales o anómalos;
- un segundo caso donde los dispositivos IoT están equipados con suficientes capacidades para realizar un análisis definitivo de comportamiento de este tipo para detectar anomalías por sí mismos.

Si bien dichos dos métodos alternativos permiten identificar cualquier amenaza para los dispositivos de IoT de forma satisfactoria, ambos métodos alternativos descritos en el documento D1 son, sin embargo, menos eficientes computacionalmente que la solución proporcionada en la presente solicitud.

En el primer caso, en la invención del documento D1, todos los datos de IoT recopilados en todos los dispositivos de IoT se tramiten al analizador (concentrador de IoT al dispositivo), lo que da como resultado un mayor tráfico de comunicaciones de red y un mayor trabajo del concentrador IoT que debe analizar todos los datos. En contraste, la invención de la solicitud es diferente a este primer caso porque envía selectivamente los datos al concentrador IoT solo tras comprobar que se ha excedido un umbral para realizar una segunda determinación donde se determina la infracción de un conjunto de reglas.

En el segundo caso, en la invención del documento D1, todos los dispositivos de IoT deben comprender recursos informáticos suficientes para realizar el análisis de comportamiento completo y definitivo de los datos de IoT localmente. En contraste, la invención de la solicitud es diferente a este segundo caso porque los dispositivos IoT **no requieren hacer un análisis definitivo** y, por lo tanto, pueden realizar análisis menos exigentes computacionalmente con menos recursos informáticos en donde el análisis definitivo lo realiza el concentrador IoT en la segunda determinación.

El documento D1 revela la realización de un análisis de comportamiento si los comportamientos observados en un dispositivo IoT son normales o anómalos, ya sea en un dispositivo analizador más potente, que recopila los comportamientos observados localmente en dispositivos IoT más simples, o en dispositivos IoT locales con capacidades suficientes para detectar anomalías.

Aunque el documento D1 menciona comparar el comportamiento observado en el dispositivo de IoT con uno o más modelos que indican un valor, por ejemplo consumo de energía normal o anormal (D1, Párrafo [0129]), en donde posiblemente también se envían los valores de umbral con los parámetros de comportamiento observados son enviados (D1, Párrafo [0130]), dichas menciones solo se refieren a una primera determinación y el documento D1, no menciona una segunda determinación, y mucho menos que dicha segunda determinación se realice con datos enviados por los dispositivos IoT, que ya han sido recibidos en el concentrador IoT y en consecuencia de la primera determinación, como lo requiere la invención que se reclama.

El párrafo [0109] del documento D1, divulga particularidades de como los analizadores generan los modelos u obtienen los datos necesarios para detectar las anomalías, pero dichos párrafos se refieren a una única determinación y no divulga ni sugiere la segunda determinación como la requiere la invención reclamada.

Aunque el párrafo [0130] del documento D1 menciona enviar los parámetros de comportamiento observado a un servicio al cliente cuando un valor observado excede un umbral, dichos servicio al cliente no puede ser considerado un concentrador IoT donde se hace una segunda determinación como la requerida en la invención de la presente solicitud. El documento D1 no menciona ni sugiere que dicho servicio al cliente haga una segunda determinación y mucho menos una determinación de si se infringió un conjunto de reglas de seguridad para el dispositivo IoT con base en los datos de IoT y en el modelo de dispositivo de IoT.

Lo anterior también se muestra en la figura 14 y al párrafo [0123] del documento D1, donde se observa que el módulo analizador 1440 reporta las anomalías al servicio al cliente 1447 pero no indica una segunda determinación (por ejemplo, no indica que dicho servicio al cliente haga alguna determinación de infracción de reglas de seguridad) ni un segundo envío de información (por ejemplo, una alerta) en consecuencia a la segunda determinación.

Particularmente, aunque el análisis de patentabilidad presentado en el oficio en referencia indica que la primera determinación de “*enviar los datos de IoT en respuesta a que se ha excedido un umbral basado en uno o más de los tipos de datos*” esta divulgada por el documento D1 en sus párrafos [0129], [0130], [0121] y [0101], y que la segunda determinación de “*si se infringió el conjunto de reglas de seguridad (593) para el dispositivo IoT*” esta divulgada por el documento D1 en su párrafo [0109], todo los párrafos se refieren a la misma determinación y no, a determinaciones diferentes como lo requiere la presente invención, por lo tanto, dichos párrafos, ni nada en el documento D1, divulgan o sugieren las dos determinaciones requerida en la invención de la presente solicitud.

En el documento D1, es claro que el análisis de los vectores de comportamiento se realiza en el ‘*módulo de análisis*’ (940, 1140, 1440) (ver párrafos [00101], [00112] y [00121] del documento D1), es decir, de acuerdo con documento D1, cualquier determinación en base al comportamiento solo se puede realizar en los dispositivos que tengan dicho ‘módulo de análisis’.

El documento D1 divulga dos realizaciones diferentes, separadas y que no se combinan entre ellas una donde el “*módulo de análisis*” (940) está en el dispositivo IoT (ver figura 9) y otras realizaciones diferentes donde el “*módulo de análisis*” (1140, 1440) está en un “*dispositivo de monitoreo*” (que el examinador toma como un concentrador de IoT) en una red local fuera del dispositivo IoT (ver figuras 11 y 14 del documento D1).

Para que la invención divulgada en el documento D1 pueda hacer las dos determinaciones que requiere la invención de la presente solicitud, se necesitaría que el “*módulo de análisis*” estuviera tanto en el dispositivo IoT, como en el concentrador IoT, pero lo divulgado en D1 enseña que dicho “*módulo de análisis*” está en el dispositivo IoT (según la figura 9 de D1) o en el “*dispositivo de monitoreo*” en una red local (según las figuras 11 y 14, y el párrafo [0128] del documento D1), pero según el documento D1, dicho módulo analizador no está en ambos. Por lo tanto, lo divulgado en el documento D1, no puede hacer una primera determinación en el dispositivo IoT, y posteriormente una segunda determinación en el concentrado de IoT porque solo tiene un “*modulo analizador*” en alguno de ellos, pero no en ambos, y de la misma forma dicha determinación se hace en el ‘*dispositivo IoT*’, o en el ‘*concentrado IoT*’, pero no en ambos.

También se indica que lo divulgado los párrafos [0129] y [0130] del documento D1 no corresponde a la presente invención porque, aunque, en dichos párrafos, se enseña que el dispositivo IoT transmite los parámetros observados a un ‘servicio al cliente’, o que el dispositivo IoT invoca una serie de mensajes con ‘asociados de soporte’ (*support partners*), el documento D1 no menciona que dicho ‘servicio al cliente’ o que dichos ‘asociados de soporte’ haga una determinación posterior para determinar, si se infringió el conjunto de reglas de seguridad y así enviar selectivamente una alerta con base en la determinación.

También se indica que lo divulgado en el párrafo [0121] del documento D1 no corresponde a la presente invención porque, aunque, en dicho párrafo, se enseña que *"la plataforma de servicio al cliente (1410) puede recibir uno o más registros de acción de los dispositivos IoT del observador (1412), (1414) además del contexto local relevante y/o información del entorno de los dispositivos IoT informativos (1416), (1418), (1420) y proporcionar los vectores de comportamiento a un módulo de análisis (1440), en el que el módulo de análisis (1440) puede agregar los vectores de comportamiento para detectar una o más anomalías de comportamiento que podrían indicar posibles ataques maliciosos, mal funcionamiento o quemaduras en los dispositivos monitoreados, u otras anomalías"*, dicho párrafo se refiere a una sola determinación, y no a una segunda determinación como lo está tomando el examinador.

Por último, se indica que lo divulgado en los párrafos [0129] y [0130] no se puede combinar con lo divulgado en el párrafo [0121] porque lo divulgado en el párrafo [0121], lo cual se basa en la arquitectura de la figura 14 (que se muestra a continuación para su rápida referencia), es diferente de base a los divulgados en los párrafos [0129] y [0130] porque los ‘dispositivos de IoT observadores’ (del párrafo [0121]) no pueden corresponder al ‘refrigerador IoT’ (de los párrafos [0129] y [0130]). Los ‘dispositivos de IoT observadores’, a diferencia del ‘refrigerador IoT’, no hace un análisis de los parámetros de comportamiento (ver párrafos [0120] y [0121]) y carecen de un ‘módulo de análisis’ (ver figura 14).

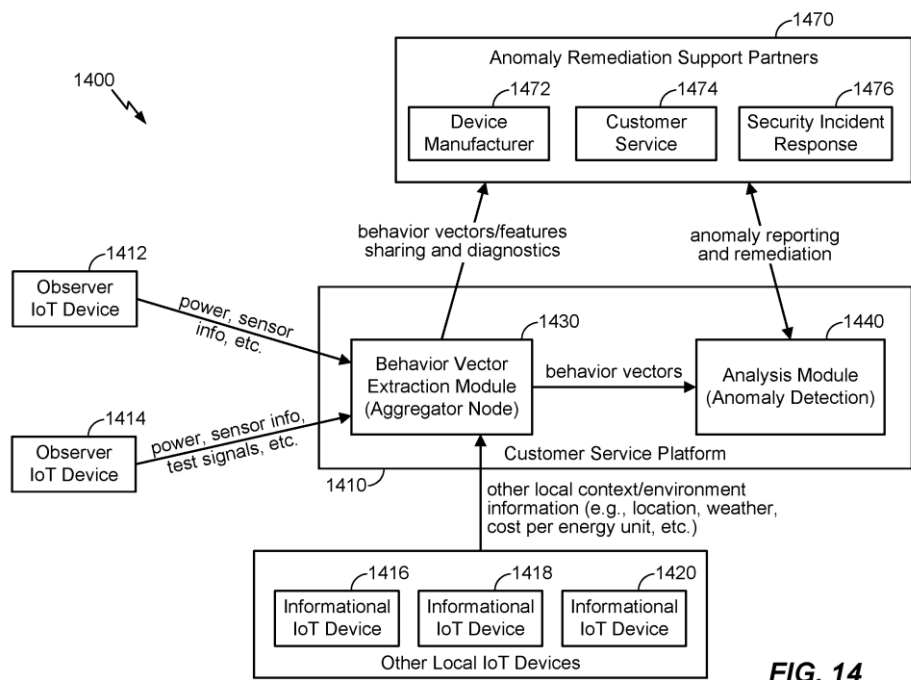


FIG. 14

Además, aunque menciona en el documento D1, lo divulgado en los párrafos [0129] y [0130] corresponde una realización en donde el “*módulo de análisis*” está en el dispositivo IoT (es decir en el ‘*refrigerador IoT*’) mientras que lo divulgado en el párrafo [0121] se refiere a una realización diferente donde el “*módulo de análisis*” está en un dispositivo análogo a un ‘*concentrador IoT*’.

Esta característica de hacer dos determinaciones en donde la segunda determinación se hace en base a los datos enviados en consecuencia a la primera determinación no es obvia ni evidente para la persona del oficio medianamente versada en la materia y, por lo tanto, esta característica no es solo nueva sino también inventiva.

Por último, se indica que inclusive, si hipotéticamente el documento D1 divulgara la dos determinaciones que requiere la invención de la presente solicitud, que como se explicó anteriormente el documento D1 no lo hace, dicho documento no divulga ni sugiere “*en donde la determinación de si se infringió el conjunto de reglas de seguridad (593) para el dispositivo IoT, la cual se basa en los datos IoT ya recibidos y ocurre a continuación después de recibir dichos datos IoT, depende de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral*” como ahora se requiere en la invención que actualmente se reclama.

El documento D1 no divulga ni sugiere dicha característica porque, en lo divulgado por el documento D1, no hay un interés en hacer, adicionalmente a un primer análisis simple (por ejemplo, la verificación de un umbral), una segunda determinación más compleja, que por su grado diferente de complejidad requiere información de otros factores a los utilizados en la primera determinación.

Por todo lo anterior se concluye que las reivindicaciones independientes en cuestión poseen características que no se dan a conocer de manera obvia para una persona versada en la materia por los documentos D1 o D2, por ende, la presente invención debe ser considerada como novedosa y con nivel inventivo sobre el estado de la técnica presentado por el Examinador.

2. Conclusión

Los argumentos expuestos en el presente escrito ponen de manifiesto de una manera clara y contundente que lo revelado en las nuevas reivindicaciones de la presente solicitud resulta completamente NOVEDOSO E INVENTIVO sobre las enseñanzas del estado del arte más cercano representado por los documentos D1 y D2, toda vez que nada dentro de dichos documentos revela en forma directa o al menos llega a sugerir todas las características que ahora se reclaman en el capítulo reivindicatorio enmendado que ahora se presenta. Por consiguiente, no se puede derivar la inexistencia de los requisitos de ley para la concesión del privilegio de patentabilidad.

En consecuencia, me permito solicitar a ese Despacho, proceder con la revisión de las modificaciones y de los argumentos aquí presentados, para conceder el privilegio de patente solicitado para la materia objeto de las 20 reivindicaciones ahora presentadas en el capítulo reivindicatorio modificado, y que de subsistir alguna duda o inquietud respecto a la patentabilidad de la presente invención, a pesar de las modificaciones y argumentos técnicos ahora presentados, sin apartarse del espíritu inventivo originalmente revelado en la solicitud internacional, se le brinde la oportunidad al solicitante de aclararla o de limitar aún más la invención, mediante la emisión de un segundo examen de fondo, teniendo en cuenta el nuevo capítulo reivindicatorio que se somete a revisión, antes de que se emita una decisión definitiva por parte de ese Despacho, de conformidad con lo dispuesto en 1.2.2.5.1 del artículo primero de la Resolución 54093 de 2012.

3. Anexos

Junto con este escrito se incluye lo siguiente:

- Capítulo reivindicatorio modificado, en donde se han llevado a cabo las modificaciones mencionadas anteriormente.

4. Pagos

Junto con esta respuesta se paga la tasa correspondiente a la modificación del capítulo reivindicatorio.

Petición

Solicito al Despacho, y en el evento que el examinador considere que pese a las modificaciones presentadas aún existen objeciones, que proceda a emitir un segundo examen de fondo sobre el nuevo capítulo reivindicatorio presentado.

En este sentido requiero se me comunique a través del SIPI o cualquier otro medio la existencia de estas objeciones para, de esta manera, si procede, realizar el nuevo pago del examen de patentabilidad de la solicitud de la referencia.

Atentamente,



LUZ HELENA ADARVE GÓMEZ.

C.C 41.575.435 de Bogotá.

T.P. 14.884 C.S.J.

FJG

P-1059

REIVINDICACIONES (con marcas de modificación)

1. Un aparato para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende:

un concentrador de IoT (351) que incluye uno o más dispositivos, los dispositivos incluyen al menos una memoria adaptada para almacenar los datos en tiempo de ejecución para los dispositivos, y al menos un procesador que está adaptado para ejecutar el código ejecutable por procesador que, en respuesta a la ejecución, permite que el concentrador de IoT (351) realice las acciones, que incluyen:

generar un modelo configurable de dispositivo de IoT;

almacenar (591) un conjunto de reglas de seguridad que están asociadas con una condición esperada de al menos un dispositivo de IoT, el conjunto de reglas de seguridad estando basado en información de operación recibida de cada uno de una pluralidad de dispositivos de IoT (341);

recibir datos de IoT (592) asociados con al menos un dispositivo de IoT (341) cuando dicho al menos un dispositivo de IoT determina enviar los datos de IoT en respuesta a que se ha excedido un umbral basado en uno o más de los tipos de datos, en donde los datos de IoT son datos agregados que incluyen al menos dos tipos diferentes de datos;

determinar, para cada dispositivo de IoT del al menos un dispositivo IoT, con base en los datos de IoT y en el modelo de dispositivo de IoT, si se infringió el conjunto de reglas de seguridad (593) para el dispositivo IoT con base en información de operación recibida de cada uno de una pluralidad de dispositivos de IoT de tal manera que la determinación está basada en una combinación de al menos dos tipos diferentes de datos de al menos dos de la pluralidad de dispositivos de IoT considerados en conjunto; y

enviar selectivamente una alerta (594) con base en la determinación;

en donde la determinación de si se infringió el conjunto de reglas de seguridad (593) para el dispositivo IoT, la cual se basa en los datos IoT ya recibidos y ocurre a continuación después de recibir dichos datos IoT, depende de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral.

2. El aparato de acuerdo con la reivindicación 1, en donde las acciones incluyen, además:

recibir una solicitud de configuración (422); y

ajustar (423) el conjunto de reglas de seguridad con base en la solicitud de configuración.

3. El aparato de acuerdo con la reivindicación 1, en donde los datos de IoT se recibe de un agente de recopilación de datos implementado en el al menos un dispositivo de IoT (341).

4. El aparato de acuerdo con la reivindicación 1, en donde el al menos un dispositivo

de IoT (341) incluye una pluralidad de dispositivos de IoT (341, 342, 343), y en donde los datos de IoT se reciben de parte de los agentes de recopilación de datos implementados en la pluralidad de dispositivos de IoT (341, 342, 343).

5. El aparato de acuerdo con la reivindicación 1, en donde el conjunto de reglas de seguridad incluye al menos una lista blanca de procesos o una lista negra de procesos.

6. El aparato de acuerdo con la reivindicación 1, en donde los datos de IoT incluyen un estado de un interruptor de manipulación en al menos un dispositivo de IoT (341).

7. El aparato de acuerdo con la reivindicación 1, en donde los datos de IoT se agregan desde múltiples dispositivos de IoT (341, 342, 343) que incluyen al menos un dispositivo de IoT (341).

8. El aparato de acuerdo con la reivindicación 1, en donde los datos agregados de los datos de IoT incluyen datos de entorno y datos de estado interno.

9. El aparato de acuerdo con la reivindicación 8, en donde los datos de entorno incluyen al menos una de temperatura, humedad, ubicación detectada o geolocalización

10. El aparato de acuerdo con la reivindicación 8, en donde los datos internos incluyen al menos uno de una versión del sistema operativo, estado actual de procesos activos, puertos abiertos o información asociada con dispositivos conectados a al menos un dispositivo de IoT (341).

11. El aparato de acuerdo con la reivindicación 1, en donde el conjunto de reglas de seguridad son de tal manera que la infracción del conjunto de reglas de seguridad indica al menos una posibilidad de un ataque, en donde el ataque es al menos uno de un ataque físico o un ciberataque en el al menos un dispositivo de IoT (341).

12. El aparato de acuerdo con la reivindicación 1, en donde enviar selectivamente una alerta con base en la determinación además incluye enviar selectivamente información sobre el ataque con la alerta.

13. Un método para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende:

generar un modelo configurable de dispositivo de IoT con base en información de operación recibida de cada uno de una pluralidad de dispositivos de IoT;

almacenar (591) un conjunto de reglas de seguridad que están asociadas con una condición esperada de al menos un dispositivo de IoT (341);

recibir los datos agregados del dispositivo de IoT (592) desde al menos un dispositivo de IoT

(341) cuando dicho al menos un dispositivo de IoT (341) determina enviar los datos de IoT en respuesta a que se ha excedido un umbral basado en uno o más de los tipos de datos, en donde los datos agregados del dispositivo de IoT incluyen al menos dos tipos diferentes de datos de la pluralidad de dispositivos de IoT;

emplear al menos un procesador para comparar los datos agregados del dispositivo de IoT con el modelo configurable de dispositivo de IoT para determinar si se ha violado el conjunto de reglas de seguridad de tal manera que la comparación se evalúa con base en una combinación de al menos dos tipos diferentes de datos de al menos dos de la pluralidad de dispositivos de IoT considerados en conjunto; ~~y~~

~~enviar selectivamente una alerta (594) con base en la comparación;~~

en donde la determinación de si se ha violado el conjunto de reglas de seguridad (593) para el dispositivo IoT, la cual se basa en los datos IoT ya recibidos y ocurre a continuación después de recibir dichos datos IoT, depende de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral; ~~y~~

~~enviar selectivamente una alerta (594) con base en la comparación.~~

14. El método de acuerdo con la reivindicación 13, en donde al menos un dispositivo de IoT (341) incluye una pluralidad de dispositivos de IoT (341, 342, 343), y en donde los datos agregados del dispositivo de IoT se reciben de parte de los agentes de recopilación de datos implementados en la pluralidad de dispositivos de IoT (341, 342, 343).

15. El método de acuerdo con la reivindicación 13, en donde los datos agregados de los datos de dispositivo IoT incluyen datos de entorno y datos de estado interno.

16. El método de acuerdo con la reivindicación 13, que comprende, además:
recibir una solicitud de configuración (422); y
ajustar (423) el modelo configurable de dispositivo de IoT con base en la solicitud de configuración.

17. Un método para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende:

emplear al menos un procesador para generar una solicitud de configuración (423), en donde la solicitud de configuración (423) es una solicitud para cambiar un conjunto de reglas de seguridad a un conjunto ajustado de reglas de seguridad, en donde el conjunto ajustado de reglas de seguridad está asociado con una condición esperada de al menos un dispositivo de IoT (341), en donde el conjunto ajustado de reglas de seguridad se basa en una evaluación de los datos de IoT asociados con cada uno de la pluralidad de dispositivos de IoT (341, 342, 343), y en donde los datos de IoT son datos agregados que son recibidos de al menos un dispositivo de IoT (341) cuando dicho al

menos un dispositivo de IoT (341) determina enviar los datos de IoT en respuesta a que se ha excedido un umbral basado en uno o más de los tipos de datos y que incluyen al menos dos tipos diferentes de datos de la pluralidad de dispositivos de IoT de manera que la aplicación del conjunto ajustado de reglas de seguridad está basado en una combinación de al menos dos tipos diferentes de datos de al menos dos de la pluralidad de dispositivos de IoT considerados en conjunto;

enviar la solicitud de configuración a un concentrador de IoT (351); y

recibir una alerta del concentrador de IoT (351) cuando el concentrador de IoT determina que se infringió el conjunto ajustado de reglas de seguridad, en donde la determinación de si se infringió el conjunto ajustado de reglas de seguridad, la cual se basa en los datos IoT ya recibidos y ocurre a continuación después de recibir dichos datos IoT, depende de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral.

18. El método de acuerdo con la reivindicación 17, en donde el conjunto ajustado de reglas de seguridad se basa en una evaluación de los datos de IoT asociados con al menos un dispositivo de IoT (341) de tal manera que al menos un dispositivo de IoT (341) sea una pluralidad de dispositivos de IoT (341, 342, 343).

19. El método de acuerdo con la reivindicación 17, en donde los datos agregados de los datos de IoT incluyen los datos de entorno y los datos internos.

20. El método de acuerdo con la reivindicación 19, donde los datos de entorno incluyen al menos una de temperatura, humedad, ubicación detectada o geolocalización, y donde los datos internos incluyen al menos uno de la versión del sistema operativo, estado actual de procesos activos, puertos abiertos, o información asociada con los dispositivos conectados a al menos un dispositivo de IoT (341).

REIVINDICACIONES

1. Un aparato para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende:

un concentrador de IoT (351) que incluye uno o más dispositivos, los dispositivos incluyen al menos una memoria adaptada para almacenar los datos en tiempo de ejecución para los dispositivos, y al menos un procesador que está adaptado para ejecutar el código ejecutable por procesador que, en respuesta a la ejecución, permite que el concentrador de IoT (351) realice las acciones, que incluyen:

generar un modelo configurable de dispositivo de IoT;

almacenar (591) un conjunto de reglas de seguridad que están asociadas con una condición esperada de al menos un dispositivo de IoT, el conjunto de reglas de seguridad estando basado en información de operación recibida de cada uno de una pluralidad de dispositivos de IoT (341);

recibir datos de IoT (592) asociados con al menos un dispositivo de IoT (341) cuando dicho al menos un dispositivo de IoT determina enviar los datos de IoT en respuesta a que se ha excedido un umbral basado en uno o más de los tipos de datos, en donde los datos de IoT son datos agregados que incluyen al menos dos tipos diferentes de datos;

determinar, para cada dispositivo de IoT del al menos un dispositivo IoT, con base en los datos de IoT y en el modelo de dispositivo de IoT, si se infringió el conjunto de reglas de seguridad (593) para el dispositivo IoT con base en información de operación recibida de cada uno de una pluralidad de dispositivos de IoT de tal manera que la determinación está basada en una combinación de al menos dos tipos diferentes de datos de al menos dos de la pluralidad de dispositivos de IoT considerados en conjunto; y

enviar selectivamente una alerta (594) con base en la determinación;

en donde la determinación de si se infringió el conjunto de reglas de seguridad (593) para el dispositivo IoT, la cual se basa en los datos IoT ya recibidos y ocurre a continuación después de recibir dichos datos IoT, depende de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral.

2. El aparato de acuerdo con la reivindicación 1, en donde las acciones incluyen, además:

recibir una solicitud de configuración (422); y

ajustar (423) el conjunto de reglas de seguridad con base en la solicitud de configuración.

3. El aparato de acuerdo con la reivindicación 1, en donde los datos de IoT se recibe de un agente de recopilación de datos implementado en el al menos un dispositivo de IoT (341).

4. El aparato de acuerdo con la reivindicación 1, en donde el al menos un dispositivo

de IoT (341) incluye una pluralidad de dispositivos de IoT (341, 342, 343), y en donde los datos de IoT se reciben de parte de los agentes de recopilación de datos implementados en la pluralidad de dispositivos de IoT (341, 342, 343).

5. El aparato de acuerdo con la reivindicación 1, en donde el conjunto de reglas de seguridad incluye al menos una lista blanca de procesos o una lista negra de procesos.

6. El aparato de acuerdo con la reivindicación 1, en donde los datos de IoT incluyen un estado de un interruptor de manipulación en al menos un dispositivo de IoT (341).

7. El aparato de acuerdo con la reivindicación 1, en donde los datos de IoT se agregan desde múltiples dispositivos de IoT (341, 342, 343) que incluyen al menos un dispositivo de IoT (341).

8. El aparato de acuerdo con la reivindicación 1, en donde los datos agregados de los datos de IoT incluyen datos de entorno y datos de estado interno.

9. El aparato de acuerdo con la reivindicación 8, en donde los datos de entorno incluyen al menos una de temperatura, humedad, ubicación detectada o geolocalización

10. El aparato de acuerdo con la reivindicación 8, en donde los datos internos incluyen al menos uno de una versión del sistema operativo, estado actual de procesos activos, puertos abiertos o información asociada con dispositivos conectados a al menos un dispositivo de IoT (341).

11. El aparato de acuerdo con la reivindicación 1, en donde el conjunto de reglas de seguridad son de tal manera que la infracción del conjunto de reglas de seguridad indica al menos una posibilidad de un ataque, en donde el ataque es al menos uno de un ataque físico o un ciberataque en el al menos un dispositivo de IoT (341).

12. El aparato de acuerdo con la reivindicación 1, en donde enviar selectivamente una alerta con base en la determinación además incluye enviar selectivamente información sobre el ataque con la alerta.

13. Un método para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende:

generar un modelo configurable de dispositivo de IoT con base en información de operación recibida de cada uno de una pluralidad de dispositivos de IoT;

almacenar (591) un conjunto de reglas de seguridad que están asociadas con una condición esperada de al menos un dispositivo de IoT (341);

recibir los datos agregados del dispositivo de IoT (592) desde al menos un dispositivo de IoT

(341) cuando dicho al menos un dispositivo de IoT (341) determina enviar los datos de IoT en respuesta a que se ha excedido un umbral basado en uno o más de los tipos de datos, en donde los datos agregados del dispositivo de IoT incluyen al menos dos tipos diferentes de datos de la pluralidad de dispositivos de IoT;

emplear al menos un procesador para comparar los datos agregados del dispositivo de IoT con el modelo configurable de dispositivo de IoT para determinar si se ha violado el conjunto de reglas de seguridad de tal manera que la comparación se evalúa con base en una combinación de al menos dos tipos diferentes de datos de al menos dos de la pluralidad de dispositivos de IoT considerados en conjunto;

;

en donde la determinación de si se ha violado el conjunto de reglas de seguridad (593) para el dispositivo IoT, la cual se basa en los datos IoT ya recibidos y ocurre a continuación después de recibir dichos datos IoT, depende de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral; y

enviar selectivamente una alerta (594) con base en la comparación.

14. El método de acuerdo con la reivindicación 13, en donde al menos un dispositivo de IoT (341) incluye una pluralidad de dispositivos de IoT (341, 342, 343), y en donde los datos agregados del dispositivo de IoT se reciben de parte de los agentes de recopilación de datos implementados en la pluralidad de dispositivos de IoT (341, 342, 343).

15. El método de acuerdo con la reivindicación 13, en donde los datos agregados de los datos de dispositivo IoT incluyen datos de entorno y datos de estado interno.

16. El método de acuerdo con la reivindicación 13, que comprende, además:
recibir una solicitud de configuración (422); y
ajustar (423) el modelo configurable de dispositivo de IoT con base en la solicitud de configuración.

17. Un método para la seguridad del internet de las cosas (IoT, por sus siglas en inglés), que comprende:

emplear al menos un procesador para generar una solicitud de configuración (423), en donde la solicitud de configuración (423) es una solicitud para cambiar un conjunto de reglas de seguridad a un conjunto ajustado de reglas de seguridad, en donde el conjunto ajustado de reglas de seguridad está asociado con una condición esperada de al menos un dispositivo de IoT (341), en donde el conjunto ajustado de reglas de seguridad se basa en una evaluación de los datos de IoT asociados con cada uno de la pluralidad de dispositivos de IoT (341, 342, 343), y en donde los datos de IoT son datos agregados que son recibidos de al menos un dispositivo de IoT (341) cuando dicho al

menos un dispositivo de IoT (341) determina enviar los datos de IoT en respuesta a que se ha excedido un umbral basado en uno o más de los tipos de datos y que incluyen al menos dos tipos diferentes de datos de la pluralidad de dispositivos de IoT de manera que la aplicación del conjunto ajustado de reglas de seguridad está basado en una combinación de al menos dos tipos diferentes de datos de al menos dos de la pluralidad de dispositivos de IoT considerados en conjunto;

enviar la solicitud de configuración a un concentrador de IoT (351); y

recibir una alerta del concentrador de IoT (351) cuando el concentrador de IoT determina que se infringió el conjunto ajustado de reglas de seguridad, en donde la determinación de si se infringió el conjunto ajustado de reglas de seguridad, la cual se basa en los datos IoT ya recibidos y ocurre a continuación después de recibir dichos datos IoT, depende de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral.

18. El método de acuerdo con la reivindicación 17, en donde el conjunto ajustado de reglas de seguridad se basa en una evaluación de los datos de IoT asociados con al menos un dispositivo de IoT (341) de tal manera que al menos un dispositivo de IoT (341) sea una pluralidad de dispositivos de IoT (341, 342, 343).

19. El método de acuerdo con la reivindicación 17, en donde los datos agregados de los datos de IoT incluyen los datos de entorno y los datos internos.

20. El método de acuerdo con la reivindicación 19, donde los datos de entorno incluyen al menos una de temperatura, humedad, ubicación detectada o geolocalización, y donde los datos internos incluyen al menos uno de la versión del sistema operativo, estado actual de procesos activos, puertos abiertos, o información asociada con los dispositivos conectados a al menos un dispositivo de IoT (341).