

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 90126

Ref. Expediente N° NC2019/0004599

Por la cual se otorga una Patente de Invención

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO (E)
en ejercicio de sus facultades legales, en especial de las conferidas en el numeral 24 del artículo 3° del Decreto 4886 de 2011, y

CONSIDERANDO

Que mediante escrito radicado en esta Superintendencia el 3 de mayo de 2019 con el N° NC2019/0004599, por LLC MICROSOFT TECHNOLOGY LICENSING, entró a fase nacional la solicitud de patente de invención titulada “SERVICIO DE SEGURIDAD DEL INTERNET DE LAS COSAS”, que corresponde a la solicitud internacional PCT/US2017/058926 del 30 de octubre de 2017.

Que la solicitud fue publicada en la Gaceta de la Propiedad Industrial N° 859 el 10 de mayo de 2019, sin que se hubieran presentado oposiciones por parte de terceros.

Que la solicitud del expediente de la referencia fue objeto de decisión en los términos del artículo 48 de la Decisión 486 de 2000 mediante la Resolución N° 55560, sobre la cual se presentó el recurso de reposición correspondiente, que fue resuelto mediante la Resolución N° 79156, en donde se decidió revocar la decisión de negación y en su lugar se ordenó dar continuidad al correspondiente trámite, en concreto adelantar un nuevo estudio de patentabilidad.

Que realizado el examen de fondo mediante Oficio No. 10562 del 8 de julio de 2022, se requirió al solicitante en los términos del artículo 45 de la Decisión 486 de la Comisión de la Comunidad Andina para que presentara respuesta a las observaciones de carácter técnico, relacionadas con la patentabilidad o cumplimiento de los requisitos establecidos por esta Decisión para la concesión de la patente.

Que el solicitante mediante escrito radicado bajo el N° NC2019/0004599 el 29 de septiembre de 2022, respondió oportunamente el requerimiento formulado sin presentar nuevo capítulo reivindicatorio. Por lo tanto, se tendrá en cuenta el capítulo reivindicatorio presentado con el radicado N° NC2019/0004599 el 24 de mayo de 2022.

Que en virtud de lo dispuesto en el artículo 14 de la Decisión 486 expedida por la Comisión de la Comunidad Andina *“Los países miembros otorgarán patentes para las invenciones, sean de producto o de procedimiento, en todos los campos de la tecnología, siempre que sean nuevas, tengan nivel inventivo y sean susceptibles de aplicación industrial.”*

Que de conformidad con los argumentos de la parte considerativa de la resolución que resolvió el recurso de reposición, esta Oficina advirtió la existencia de documentos anteriores a la fecha de prioridad reivindicada para la determinación del estado de la técnica, situación que podría tener alguna incidencia en el desarrollo del examen de patentabilidad, por lo cual, se procederá realizar el análisis correspondiente sobre cada uno de ellos, de la siguiente manera:

El documento US20150163121 no divulga la determinación de la violación con información ya recibida e inmediatamente después de recibirla, por el contrario, este documento requiere



Resolución N° 90126

Ref. Expediente N° NC2019/0004599

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.

El documento US20160212099 no se refiere a que la determinación de la infracción de reglas de seguridad dependa de otros factores a los utilizados en la determinación de enviar los datos de IoT en respuesta a que se ha excedido el umbral.

Que en el presente caso dichas reivindicaciones cumplen los requisitos indicados en el considerando anterior, toda vez que se refieren a un aparato y métodos para servicio de seguridad del internet de las cosas, que difieren de la información del estado de la técnica más cercano, WO2016140912, en que la invención incluye una determinación, 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; una determinación, 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 para el dispositivo IoT; y una determinación de si se infringió el conjunto de reglas de seguridad 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.

Adicionalmente, estas diferencias no se encuentran sugeridas en el estado de la técnica y, como consecuencia de ello, se evidencia el efecto técnico de garantizar un nivel alto de seguridad para los dispositivos IoT de una manera más eficiente ya que se reduce la cantidad de información enviada por los canales de comunicaciones.

En consecuencia, las reivindicaciones 1 a 20 cumplen los requisitos de novedad, nivel inventivo y aplicación industrial establecidos en la normatividad citada en precedencia y esta Oficina encuentra procedente conceder para las mismas la patente solicitada.

Que de acuerdo con la modificación presentada por el solicitante en el escrito radicado bajo el N° NC2019/0004599 el 15 de septiembre de 2020 y teniendo en cuenta el objeto concedido, se modifica el título de la invención el cual quedará de la siguiente manera: “APARATO Y MÉTODOS PARA SERVICIO DE SEGURIDAD DEL INTERNET DE LAS COSAS”.

Con fundamento en las anteriores consideraciones, el Superintendente de Industria y Comercio (E),

RESUELVE

ARTÍCULO 1: Otorgar patente de invención a la solicitud que entró en fase nacional en virtud del Tratado de Cooperación en Materia de Patentes (PCT), para la creación titulada:

“APARATO Y MÉTODOS PARA SERVICIO DE SEGURIDAD DEL INTERNET DE LAS COSAS”

Clasificación IPC: H04L 29/06, G06F 21/55, H04W 4/00, H04L 12/26

Reivindicación(es): 1 a 20 incluidas en el radicado bajo el N° NC2019/0004599 el 24 de mayo de 2022, de acuerdo con el Anexo No. 1

Titular(es): LLC MICROSOFT TECHNOLOGY LICENSING.

Resolución N° **90126**

Ref. Expediente N° NC2019/0004599

Dirección(es): ONE MICROSOFT WAY, REDMOND, WASHINGTON, 98052-6399, ESTADOS UNIDOS DE AMÉRICA

Inventor(es): Arjmand SAMUEL.

Prioridad(es) N°: 4/11/2016, US (ESTADOS UNIDOS DE AMÉRICA), 15/344,461.

Solicitud internacional N°: PCT/US2017/058926

Fecha: 30 de octubre de 2017.

Vigente desde: 30 de octubre de 2017

Hasta: 30 de octubre de 2037.

ARTÍCULO 2: El titular tendrá los derechos y las obligaciones establecidos en la Decisión 486 de la Comisión de la Comunidad Andina y en las demás disposiciones legales vigentes sobre propiedad industrial, precisando que para mantener vigente la patente se deberá cancelar la tasa anual de mantenimiento, conforme lo dispone el artículo 80 de la referida norma comunitaria.

ARTÍCULO 3: Notificar el contenido de la presente resolución a LLC MICROSOFT TECHNOLOGY LICENSING, advirtiéndole que contra ella procede el recurso de reposición, ante el Superintendente de Industria y Comercio (E), el cual podrá ser interpuesto en el momento de la notificación o dentro de los diez (10) días hábiles siguientes a ella.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., el 21 de diciembre de 2022

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO (E),



Firmado digitalmente
por: JUAN CAMILO
DURAN TELLEZ
Fecha: 2022.12.21
12:02:03 COT
Razón: Validez jurídica.
Ubicación: Bogotá,
Colombia.

Resolución N° 90126

Ref. Expediente N° NC2019/0004599

ANEXO No. 1**REIVINDICACIONES CONCEDIDAS**

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.

Resolución N° 90126

Ref. Expediente N° NC2019/0004599

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

Resolución N° 90126

Ref. Expediente N° NC2019/0004599

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).