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.

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 procesoso 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 en cuanto a si se ha violado el conjunto de reglas de seguridad de tal manera que la comparación se evalua 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.

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.

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).