SEGURIDAD EN INTERNET DE LAS COSAS

Proyecto de grado

Estudiantes:

Daniel Felipe Tarquino Murgueito

Edwin Sebastian Garcia Garcia

Directores:

Claudia Patricia Santiago Cely

Daniel Orlando Díaz López

Ingeniería de Sistemas

Bogotá D.C

Julio de 2017

Tabla de contenido

1. GLOSARIO

Internet de las cosas:

El internet de las cosas se entiende como “un paradigma que se ve aplicado en las telecomunicaciones inalámbricas modernas”. Y tiene por objetivo, estar presente en casi todo lo que nos rodea (cosas u objetos), como identificación por tarjetas, etiquetas, sensores, celulares, neveras y demás. Estos son capaces de interactuar entre sí y cooperar con su red, con el fin de alcanzar objetivos comunes. Estos objetivos comunes son, por lo general, recopilar datos de diferentes fuentes (en este caso todos los objetos), con el fin de consolidarlos y darles sentido y así brindar información sobre un entorno específico.

2. INTRODUCCIÓN

El internet de las cosas es una tecnología que está en auge y lo estará por un par de años más, sin embargo, no se piensa nuca si existen fallas de seguridad, ya que solo nos preocupa a funcionalidad y nunca si alguien por debajo se esté robando nuestra información, es por eso que este trabajo trata de la seguridad en el internet de las cosas, haciendo un análisis (Se realizó en 2 artículos.) e implementaciones que están detalladas en los manuales.

Sabemos que esta tecnología trae facilidades en distintitas áreas y dentro de estas en distintos niveles, por eso que en las áreas se vieron los tipos de vulnerabilidades y las posibles amenazas y luego de este análisis plantear posibles acciones que logren mitigar o de ser posible eliminar el riesgo para así poder disfrutar esta tecnología de una manera mas segura.

3. DESCRIPCIÓN DEL PROYECTO

3.1. OBJETIVOS

3.1.1. OBJETIVO GENERAL

Realizar una revisión de escenarios de aplicación de Internet de las Cosas (IoT) para identificar riesgos de seguridad sobre elementos fundamentales de la arquitectura IoT y así definir mecanismos de protección oportunos que prevengan la materialización del riesgo o disminuyan el impacto asociado en caso de ocurrencia.

3.1.2. OBJETIVOS ESPECÍFICOS

A. Evaluar alternativas tecnológicas, las cuales permitan realizar la implementación de los criterios de seguridad definidos.

B. Implementar la solución propuesta, a través de un escenario seleccionado, aplicando por medio de una plataforma tecnológica, la evaluación del cumplimiento de los criterios de seguridad establecidos.

C. Realizar pruebas de funcionalidad y generar una conclusión al respecto.

3.2. PLANTEAMIENTO DEL PROBLEMA

Hoy por hoy, el concepto de Internet de las Cosas, es algo que está inmerso en muchos aspectos de nuestra vida cotidiana. Básicamente, Internet de las Cosas, abarca a todos aquellos dispositivos conectados a la red, que constantemente están generando información, para su posterior análisis y así resolver muchas necesidades y problemas, pero todo este tratamiento de información es delicado, pues esta información se está generando a diario, pero no se tiene la certeza de que se está haciendo con ella o quien la puede utilizar. Es por esto, que se debe pensar en el aspecto de seguridad, para así garantizar la protección de esta información y de los componentes que hacen parte del sistema de Internet de las Cosas.

3.3. JUSTIFICACIÓN

Las soluciones tecnológicas fundamentadas en dispositivos IoT son cada vez más comunes y se encuentran en escenarios de aplicación tales como entornos de producción industrial, redes vehiculares, ciudades inteligentes, gestión del medio ambiente, apoyo a procesos de aprendizaje, servicios médicos electrónicos, domótica, e incluso servicios bancarios. Tener dispositivos IoT que interactúan y se conectan con otros elementos en internet permite soñar con un conjunto de nuevos servicios y aplicaciones que puedan resolver problemas y necesidades de nuestras sociedades, sin embargo, estas nuevas soluciones deben revisarse desde una perspectiva de seguridad con el fin de que se garantice la protección de los datos gestionados y de los componentes propios de una arquitectura IoT. La definición de mecanismos de protección que hagan frente a los posibles riesgos de seguridad de estos escenarios permitirá tener servicios funcionales de alta utilidad en los que los usuarios puedan confiar.

4. ALCANCE DEL PROYECTO

El proyecto inicialmente buscó, la identificación de los escenarios, en lo que IoT tiene mayor impacto. Luego se seleccionó uno de estos escenarios y se determinó las amenazas de seguridad que estas pueden presentar, para así plantear e implementar una serie de soluciones, que puedan atacar estas amenazas y así aportar al buen desarrollo del escenario seleccionado.

Posteriormente se realizó una familiarización con 10 plataformas tecnológicas, orientadas a IoT, para que, de esta manera, se tuviera certeza de la selección de las dos plataformas más completas y a través de ellas, se realizó la implementación de un escenario IoT, con el cual se realice una comparación de las herramientas, y así analizar cual plataforma cubre la mayoría de criterios de seguridad, que se establecieron. Para ello, también se realizó una serie de pruebas, las cuales garantizan la funcionalidad de dicho escenario.

5. MARCO TEÓRICO Y ESTADO DEL ARTE

Internet de las Cosas es un concepto que se refiere a la interconexión digital de objetos cotidianos, con internet.

El internet de las cosas debería codificar entre 50 a 100 000 billones de objetos, y seguir interactuando con estos. Realizando un cálculo, se estima que el ser humano está rodeado de al menos 1000 a 5000 objetos. Según la empresa Gartner en 2020 habrá en el mundo aproximadamente 26 millones de dispositivos que estén dentro del concepto de internet de las cosas. Por otra parte, Abi Research afirma que para el mismo año habrá 30 millones de dispositivos inalámbricos conectados a internet.

Por otra parte, un estudio revela que 90% de los dispositivos IoT posee problemas de privacidad, mientras que un 70% no encripta los datos.

Volviendo a la cantidad de dispositivos que se planea tener en un futuro, se dice que el crecimiento de estos, agudizara los problemas de seguridad y de privacidad, pues estos dispositivos son capaces de realizar un procesamiento limitado y no son capaces de ejecutar soluciones antimalware convencionales. Lo cual puede incrementar el robo de datos en cualquier ámbito, y muchas veces este robo es la prioridad para los hackers.

6. METODOLOGÍA PROPUESTA

6.1. METODOLOGÍA PARA PROYECTO DE GRADO 1

A. Se llevó a cabo una investigación de escenarios generales, en los cuales el uso de IoT es importante.

B. Luego, se realizó una investigación de diez escenarios puntuales, en los cuales se determinan las tecnologías que se utilizan, así como también se identificaron las vulnerabilidades, riesgos y amenazas.

C. Una vez planteados los riesgos y las amenazas, se hizo una estimación del impacto que cada uno de estos puede generar, basándonos en que el impacto está determinado por:

IMPACTO = AMENAZA X RIESGO

D. Una vez planteado el nivel de impacto para cada amenaza, se plantea una serie de soluciones, que mitiguen el impacto de estas amenazas.

E. Después de haber realizado la propuesta de las soluciones, se llevó a cabo nuevamente el proceso descrito en el numeral C. Para así ver, cual es la solución que más impacto genera en el escenario.

F. Una vez identificada la solución más viable, se buscó llevarla a cabo con ayuda de la herramienta openIoT.

G. Llevada a cabo esta solución en la herramienta, se buscó hacer una serie de pruebas, en las cuales se vea el óptimo funcionamiento de la solución planteada.

6.2. METODOLOGIA PARA PROYECTO DE GRADO 2

A. Se definieron los principales criterios de seguridad, que se deben cubrir en el escenario.

B. Luego, investigaron las principales plataformas tecnológicas, que permitan desarrollar la simulación del escenario seleccionado.

C. Para cada una de estas plataformas, se desarrolló una familiarización, la cual tuvo por objetivo definir que plataforma cubre la mayoría de los criterios que se definieron en el numeral A.

D. Una vez, realizada esta familiarización, se seleccionaron las dos plataformas más completas, para que en ellas se pudiera realizar la simulación del escenario establecido.

E. Llevar a cabo la simulación del escenario establecido.

F. Teniendo el escenario establecido, se realizaron las pruebas de funcionalidad y seguridad, para verificar que se cubran los principales criterios de seguridad.

7. TRABAJO DESARROLLADO

Como se explica en la metodología en proyecto de grado uno, se hizo un artículo de investigación en donde se hizo énfasis en los campos a los cuales se aplica la tecnología internet de las cosas, este énfasis consistió en la revisión de 10 escenarios generales, en los cuales se está implementando el internet de las cosas. Después de haber propuesto estos 10 escenarios, se pasó a profundizar en cada uno de ellos. Para ello, lo que se hizo, fue una investigación de 1 escenarios más específico, por cada uno de los escenarios generales. Es decir que al final se reunieron un total de 10 escenarios específicos. Hay que resaltar, que un paso importante que se tuvo en cuenta, fue que se plantearon las principales amenazas que pueden ocurrir en los escenarios planteados, posterior a esto se plantearon una serie de posibles soluciones. Esto último se sometió a evaluación, para así determinar la posibilidad de ocurrencia, de cada una de estas amenazas, y las soluciones que se pueden implantar para esta amenaza.

Finalmente, se realizó una implementación en la plataforma **OpenIoT.** El manual que se siguió para realizar esta implementación se encuentra en esta URL https://github.com/OpenIoTOrg/openIoT/wiki/VDKv2---OpenIoT-Release-0.6.1---Virtual-Box-Setup-Guide

En proyecto de grado dos, se realizó un artículo analizando varias plataformas internet de las cosas, de las cuales se eligieron dos. A continuación, se pensó en realizar una implementación dentro de un tema especificó de alguna industria. Recientemente, había ocurrido la tragedia del avión del equipo de fútbol brasileño, Chapecoense, lo cual generó una oportunidad, en la cual se busca, que por medio de internet de las cosas, se puedan evitar esta serie de incidentes, dentro de la industria aeronáutica. Para ello, se realizó una simulación de vuelo en dos plataformas de las escogidas, Samsung Artik y Watson IoT. En donde se crearon los siguientes sensores

1. Dispositivo de gestión de colisiones: Dispositivo IoT que mide dos valores: i) presencia de objetos dentro de un espacio horizontal y ii) presencia de objetos dentro de un espacio vertical.
2. Dispositivo de gestión de presión en cabina: Dispositivo IoT que mide un valor: i) Nivel de Presión interna de la cabina. Como actuador tiene la capacidad de regular el nivel de presión.
3. Dispositivo de gestión de altitud: Dispositivo IoT que mide un valor: i) Altitud del avión.
4. Dispositivo de gestión de nivel de combustible: Dispositivo IoT que mide un valor: i) Nivel de combustible.
5. Dispositivo de gestión de temperatura de motor: Dispositivo IoT que mide un valor: i) Temperatura del motor.
6. Dispositivo de gestión de líquido refrigerante para motor: Dispositivo IoT que mide un valor: i) Nivel del líquido refrigerante del motor del avión. Como actuador tiene la capacidad aumentar o disminuir la cantidad de líquido.

7. Dispositivo de detección de tormentas: Dispositivo IoT que mide dos valores: i) Distancia hacia una tormenta y ii) severidad de la tormenta.
8. Dispositivo de detección de fuego: Dispositivo IoT que mide un valor: i) Existe fuego o no. Como actuador tiene la capacidad de rosear espuma retardarte de llama.
9. Sistema de navegación: Dispositivo IoT que detecta la latitud y longitud del avión (posición).

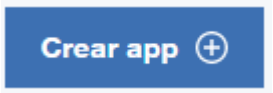
Y se mostraba en tiempo real el funcionamiento de los mismos.

7.1. TRABAJO DESARROLLADO EN IBM WATSON IoT

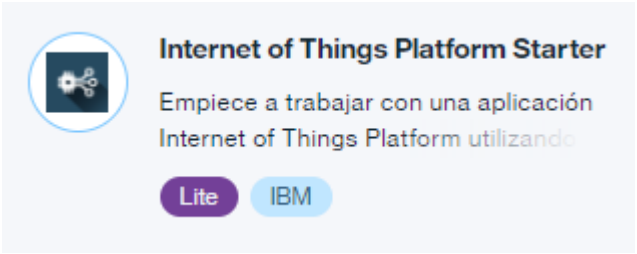
El siguiente manual va a describir como se realizaron los sensores simulados, y como se conectaron a la aplicación Watson IoT para su respectiva interpretación de datos.

A. Crear una cuenta en Bluemix
   a. https://console.bluemix.net/registration/?target=%2Fdashboard%2Fapps
   b. Se creará una cuenta gratuita, después de 30 días deberá ingresar una tarjeta de crédito para poder acceder a sus proyectos.

B. Una vez adentro crearemos una nueva app en el siguiente botón



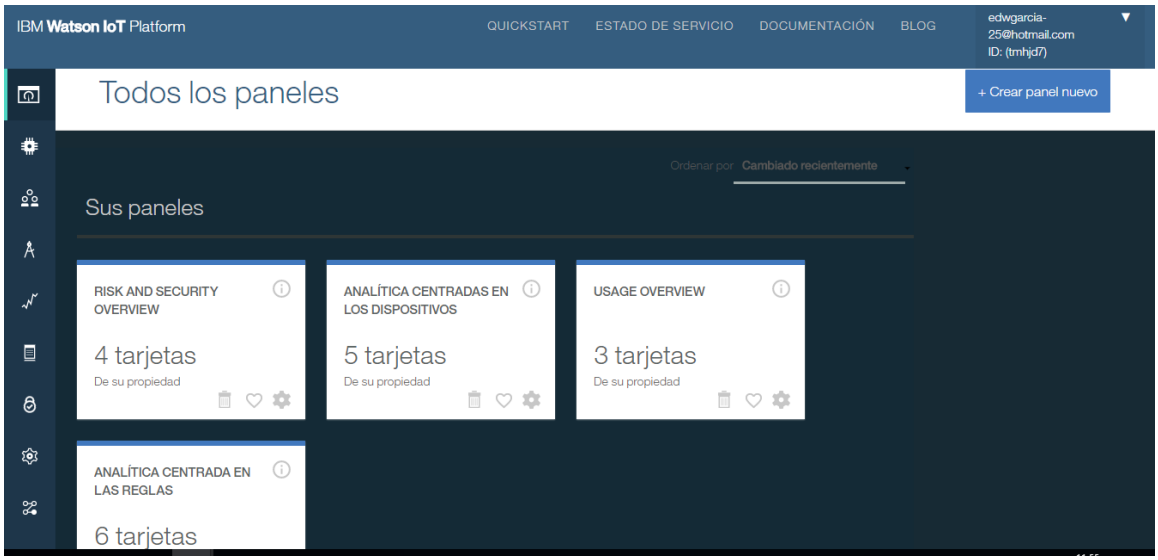
   a. Y seleccionamos la opción *Internet of Things Platform Started*



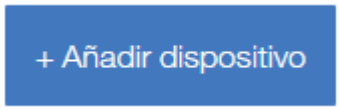
   b. En donde daremos un nombre a la aplicación y damos crear.

C. Dentro del proyecto damos en *Watson IoT Platform* y damos *Launch* eso nos redirigirá a la página de Watson IoT

a.

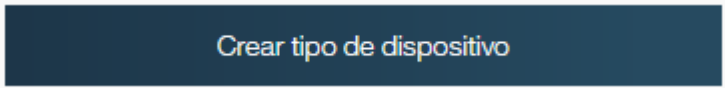


D. En la pestaña dispositivos seleccionamos *Añadir dispositivo*



a. Seleccionamos *Crear tipo de dispositivo*

b.



c. En la siguiente ventana dar el mismo botón

d. En la ventana *Crear tipo de dispositivo* dar el nombre del tipo de dispositivo a conectar y una descripción, para evitar confusiones lo llamaremos como el tipo de dispositivo. Ej: Sensor Tormenta.

e. Luego de la creación del mismo se redirigirá a la ventana de *Añadir dispositivo* se selecciona el tipo que se creó y siguiente.

f. Pedirá asignar un ID, aquí asignaremos el nombre del sensor. Ej: Sensor Tormenta.

g. Después de esto pedirá asignar una clave o se asignará automáticamente, se recomienda asignarla a mano.

h. Si se realizó bien el proceso aparecerá una ventana donde indique las características, estas hay que tenerlas presentes para configurarlas en el servidor. Esto se explicará a continuación.

i.

ID de organización	tmhjd7
Tipo de dispositivo	Tormenta
ID de dispositivo	SensorTormenta
Método de autenticación	token
Señal de autenticación	123456789

E. Para crear la simulación estos se subieron a un repositorio y se instalaron en un Ubuntu server (Puede hacerse en cualquier otro sistema operativo, pero aquí se trabajó con Ubuntu Server)

F. En la maquina ingresar los siguientes comandos

- **a.** $mkdir “Nombre de carpeta” - Esto para crear a carpeta donde se contendrá todo el proyecto
- **b.** $cd “Nombre de carpeta” - esto para entrar a la carpeta
- **c.** $git clone “Aquí va la URL del repositorio (Se encuentran más abajo)”
- **d.** $ cd device-simulator-for-ibm-IoT – Esto para entrar a una carpeta dentro del archive clonado
- **e.** $ npm install – Esto instalara el componente que hará que funcione la conexión
- **f.** $ cp. env.example .env – Aquí se copia un archivo que se necesita para la configuración
- **g.** $ nano. env – Se van a configurar los datos del sensor a conectar (Los de la imagen del punto anterior)
    1. IoTf_org=<ID de organización>
    2. IoTf_type=<Tipo de dispositivo>
    3. IoTf_id=<ID de dispositivo>
    4. IoTf_authtoken=<Señal de autenticación>
    5. control-x, Y, <enter> - Con esto se guardará y se saldrá del archivo
- **h.** $node app.js – A través de este comando se ejecutará la aplicación

- **i.** Se crearon los siguientes sensores, aquí están sus características y el link donde se encuentra el repositorio

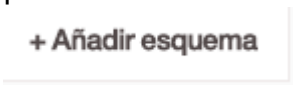
- **j.** Dispositivo de gestión de colisiones: Dispositivo IoT que mide dos valores: i) presencia de objetos dentro de un espacio horizontal y ii) presencia de objetos dentro de un espacio vertical. https://github.com/edwgarcia25/colisiones
- **k.** Dispositivo de gestión de presión en cabina: Dispositivo IoT que mide un valor: i) Nivel de Presión interna de la cabina. Como actuador tiene la capacidad de regular el nivel de presión. https://github.com/edwgarcia25/presion

l. Dispositivo de gestión de altitud: Dispositivo IoT que mide un valor: i) Altitud del avión. https://github.com/edwgarcia25/sensor-altura
m. Dispositivo de gestión de nivel de combustible: Dispositivo IoT que mide un valor: i) Nivel de combustible: https://github.com/edwgarcia25/vitrina (Aquí también se encuentra el sensor de distancia)
n. Dispositivo de gestión de temperatura de motor: Dispositivo IoT que mide un valor: i) Temperatura del motor. https://github.com/edwgarcia25/tempMotor
o. Dispositivo de gestión de líquido refrigerante para motor: Dispositivo IoT que mide un valor: i) Nivel del líquido refrigerante del motor del avión. Como actuador tiene la capacidad aumentar o disminuir la cantidad de líquido. https://github.com/edwgarcia25/liquido
p. Dispositivo de detección de tormentas: Dispositivo IoT que mide dos valores: i) Distancia hacia una tormenta y ii) severidad de la tormenta. https://github.com/edwgarcia25/tormenta
q. Dispositivo de detección de fuego: Dispositivo IoT que mide un valor: i) Existe fuego o no. Como actuador tiene la capacidad de rosear espuma retardarte de llama. https://github.com/edwgarcia25/fuego
r. Sistema de navegación: Dispositivo IoT que detecta la latitud y longitud del avión (posición). https://github.com/edwgarcia25/posicion

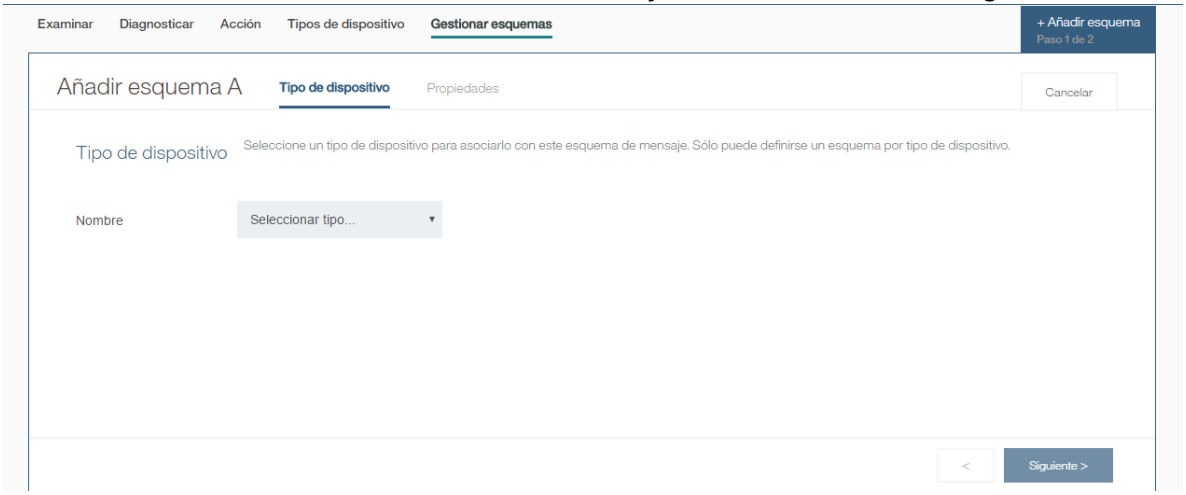
G. Nota: De no encontrarse habilitadas las URL's, dentro de este cd se encuentran cada uno se los sensores configurados

H. Una vez realizada la configuración de los sensores a la plataforma al omento de ejecutarlo si se realizó bien el proceso se tendrá que mostrar en la pestaña de *Dispositivos* los sensores emitiendo esta señal 

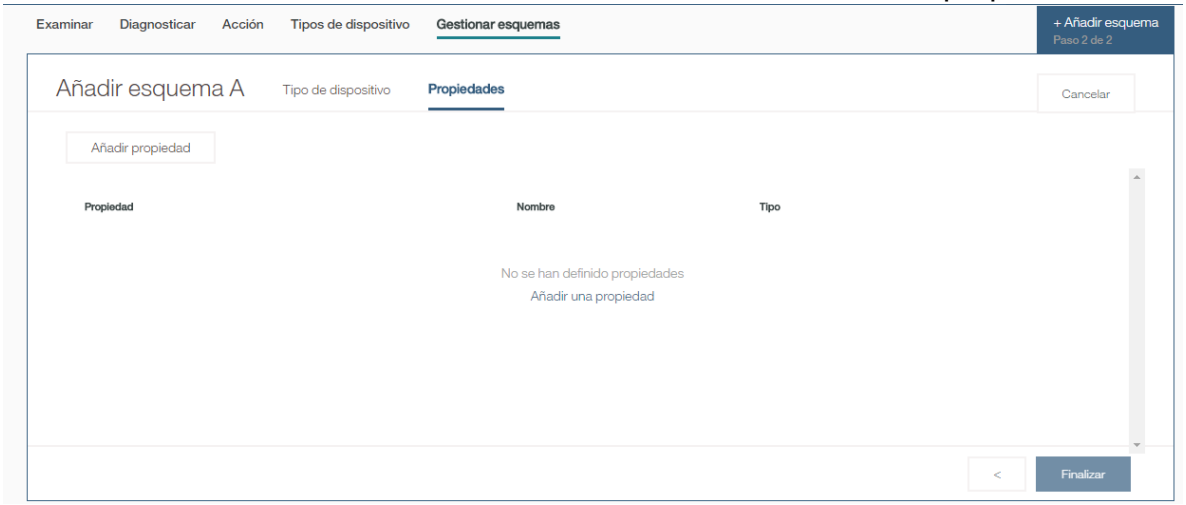
I. Ahora la aplicación tiene la opción de crear reglas, esto para avisar cuando un dato no corresponde al que debería leer, para esto hay que crear unas propiedades primero. Esto en la pestaña *Dispositivos* y dentro de esta en la pestaña *Gestionar esquemas* en donde el botón *Añadir esquema*



J. Dentro de esta ventana seleccionaremos el tipo de dispositivo, aparecerá la lista de los creados y damos siguiente

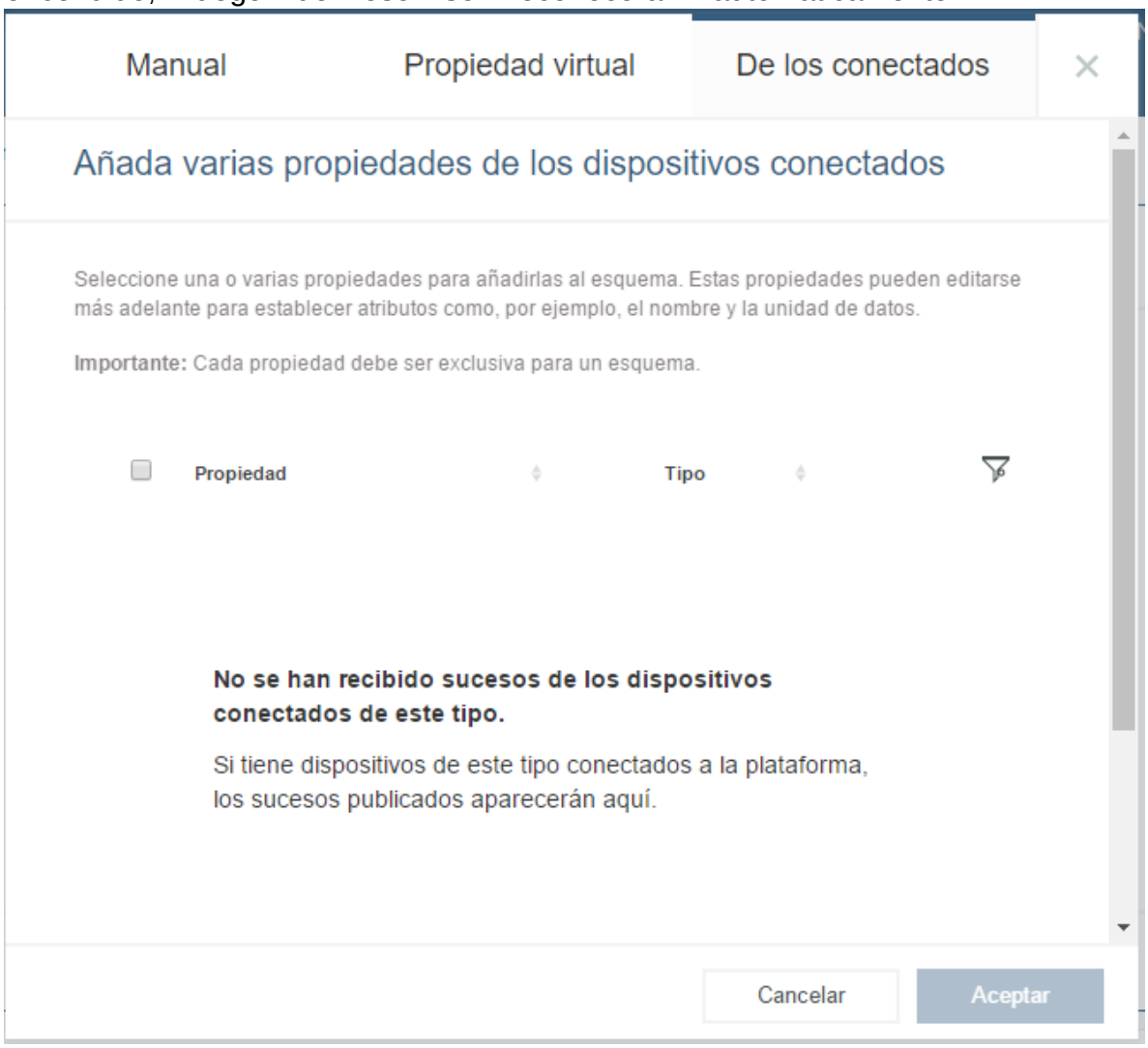


K. Dentro de esta ventana damos en el link de añadir propiedad



a. En la cual abrirá la siguiente ventana, donde se dará en la pestaña *De los conectados*. Para que recia sucesos el sensor debe estar

encendido, luego de eso se reconocerán automáticamente.



L. Ahora se da clic en a pestaña *Reglas* y le damos al botón *Crear una regla de nube*

a.

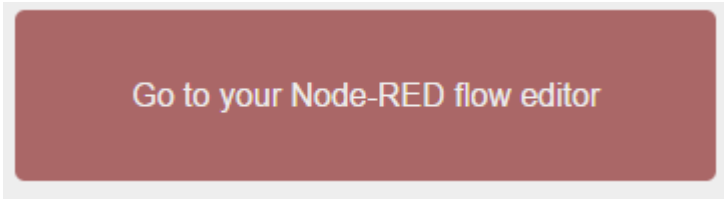
b. Una vez damos a este botón abrirá la siguiente ventana

c. Donde se asignará un nombre para la regla y en donde dice *Se aplica a:* se selecciona el esquema que se creó con anterioridad.

M. Luego de dar *Siguiente* se abrirá una ventana de este tipo

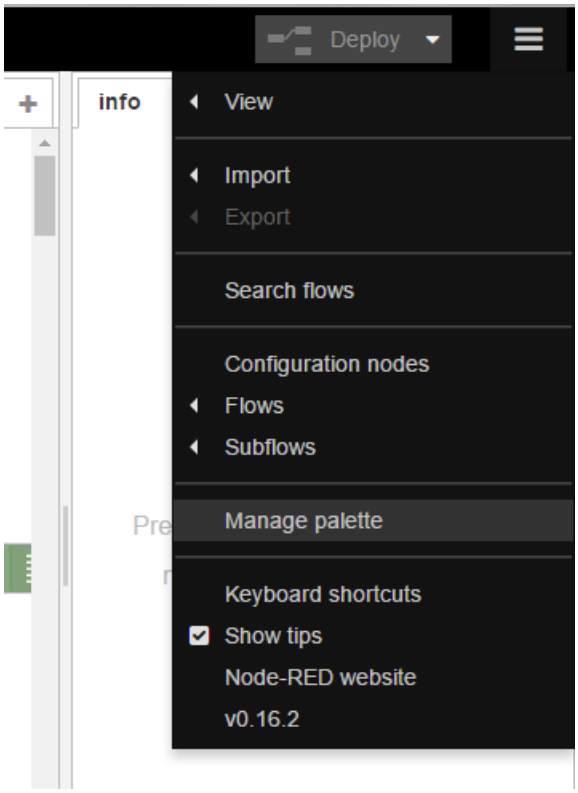
a. Al lado izquierdo vamos a crear la regla y al lado derecho la acción que hará. Al crear la condición solo se selecciona la propiedad a comparar y contra que se hará la comparación, y al crear la acción se selecciona la opción de correo electrónico y se ingresa el mensaje y el correo donde se enviará. De cumplirse la regla, al correo inscrito llegara la información de porque se cumplió la regla.

N. Para graficar vamos de nuevo a Bluemix donde se encuentran las aplicaciones y damos clic en el link que se encuentra allí y dentro de la misma damos clic a este botón



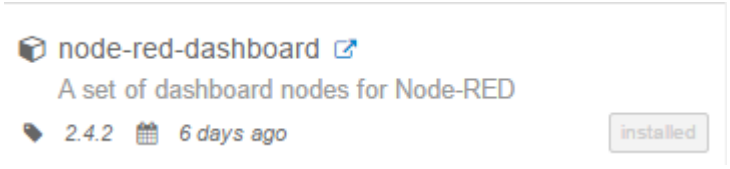
O. Una vez dentro del editor vamos a seleccionar *Manage palette* de la siguiente forma

a.



b. Y en la pestaña *Install* ingresamos la palabra *dashboard* e instalamos el siguiente complemento

c.



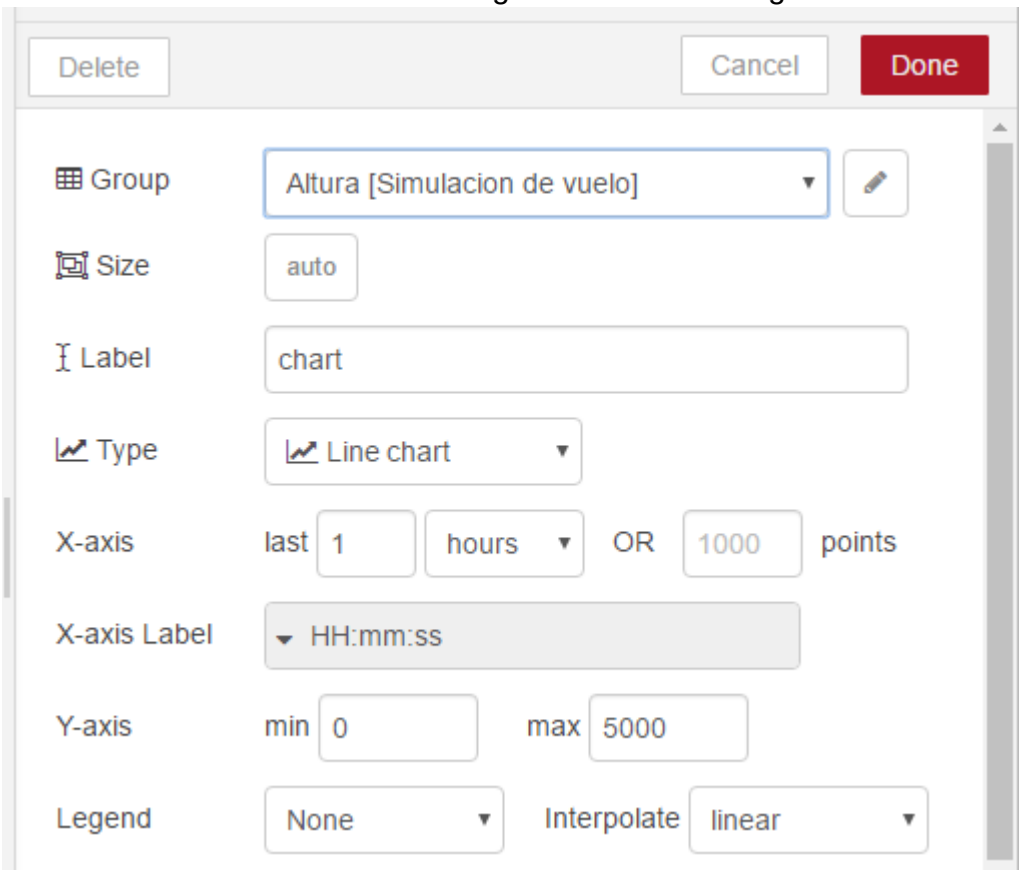
P. Ahora dentro del nodo de función pegamos la siguiente línea

a. *return {payload:msg.payload.d.altura};*

b. Esto en el caso de trabajar con el sensor de altura, luego en la lista de nodos buscamos el nodo *chart*

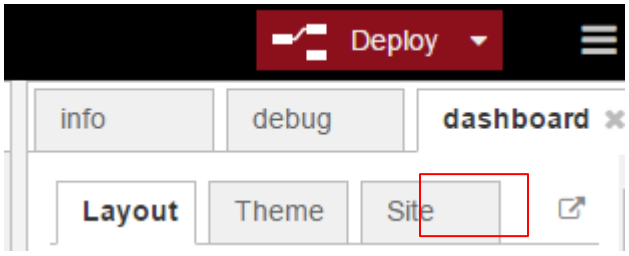
c.

d. Y dentro del nodo lo configuramos dela siguiente forma

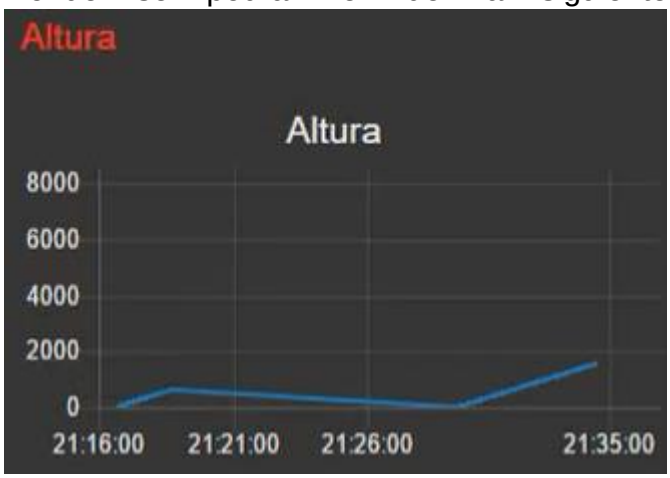


Q. Ahora en la pestaña *Dashboard* damos clic al botón que muestra la imagen para que nos lleve a la página donde se está graficando en tiempo real la información del sensor.

a.



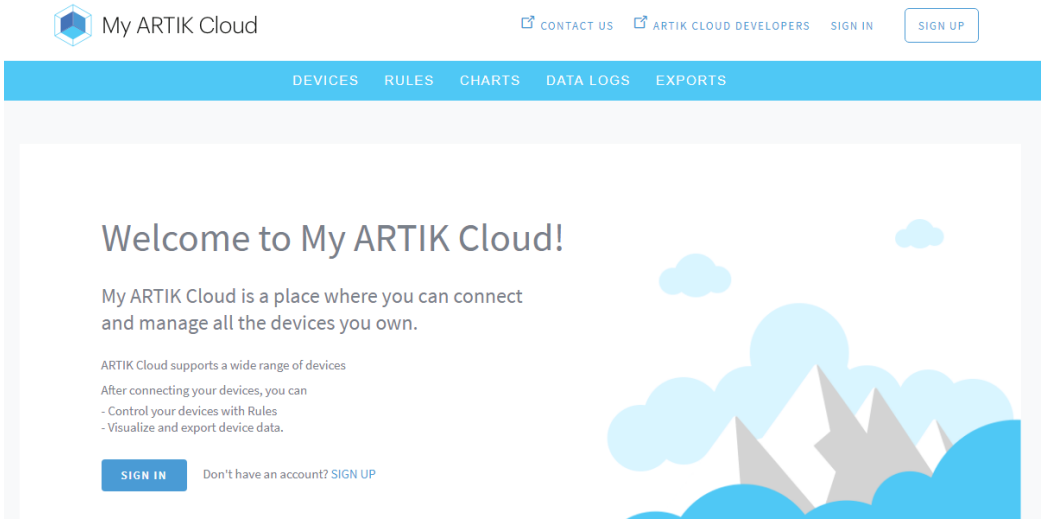
b. Donde se podrá ver de la siguiente forma la gráfica.



7.2. TRABAJO DESARROLLADO EN SAMSUNG ARTIK

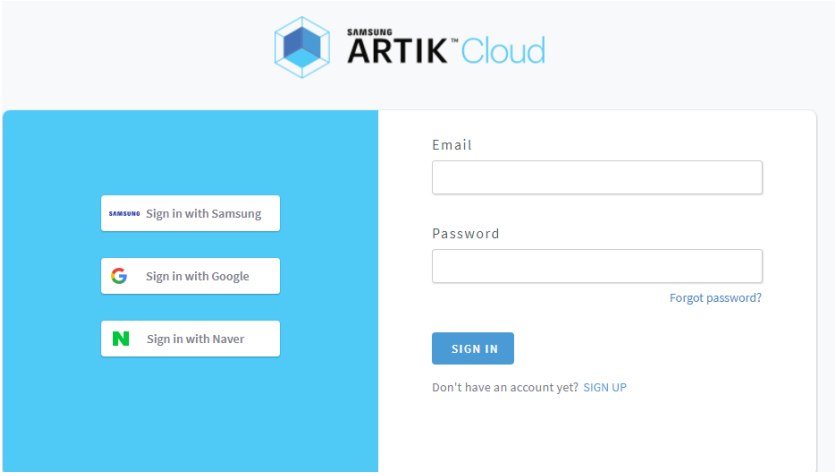
A continuación, se expondrán los pasos que se deben realizar para la creación de un sensor en la nube de Samsung Artik.

A. Se debe ingresar a la siguiente URL https://my.artik.cloud/ la cual nos mostrará la siguiente pantalla:

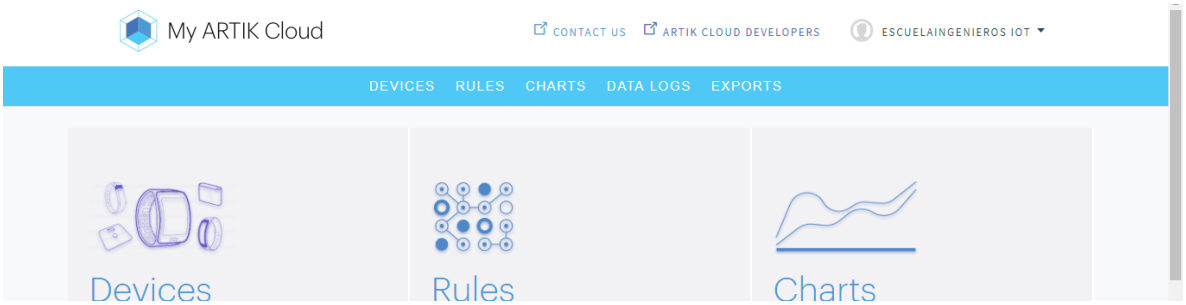


Se debe dar clic en Sign In

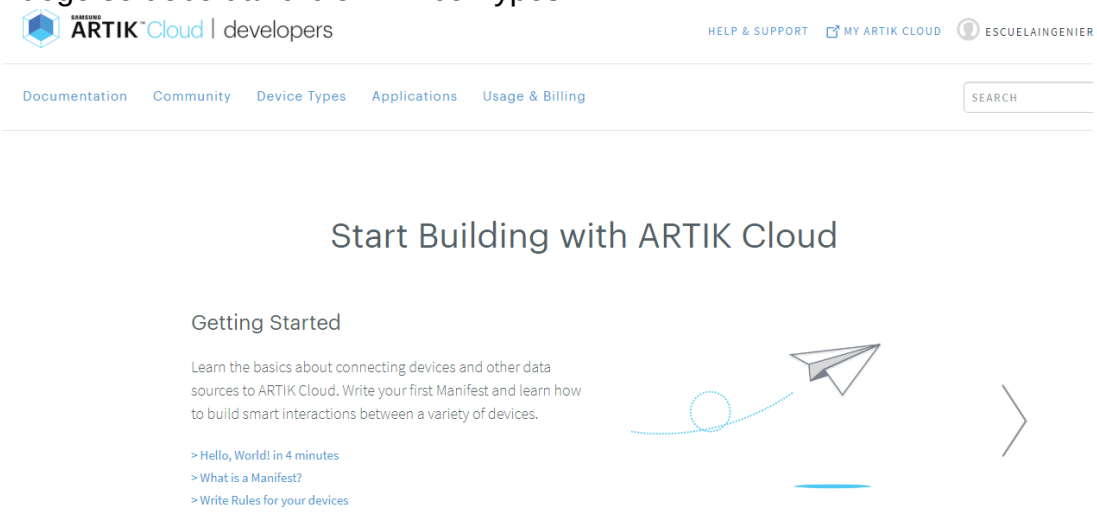
B. Se selecciona un método de autenticación, en este caso, con una cuenta de Google.



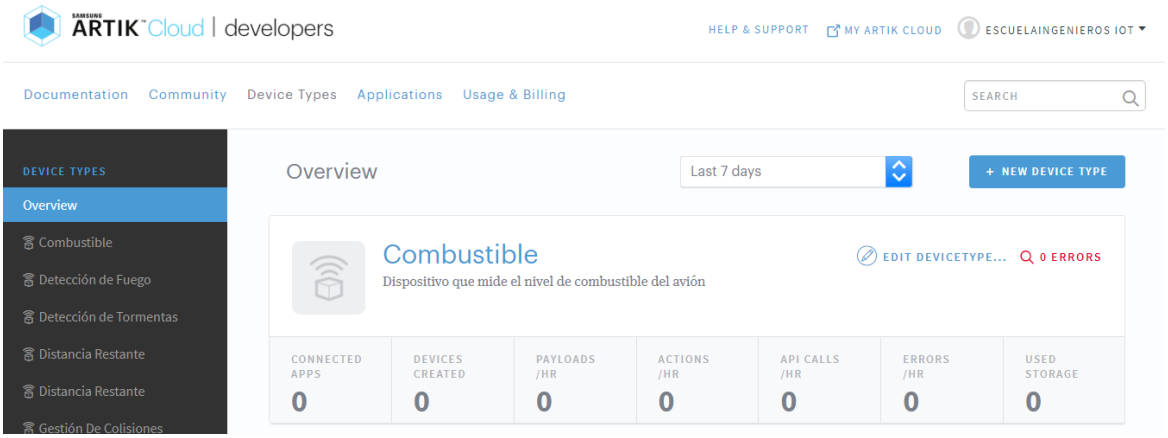
C. Después de haber hecho la autenticación, se debe dirigir a Artik Cloud Developers, dando clic en la parte superior, como se muestra en la imagen.



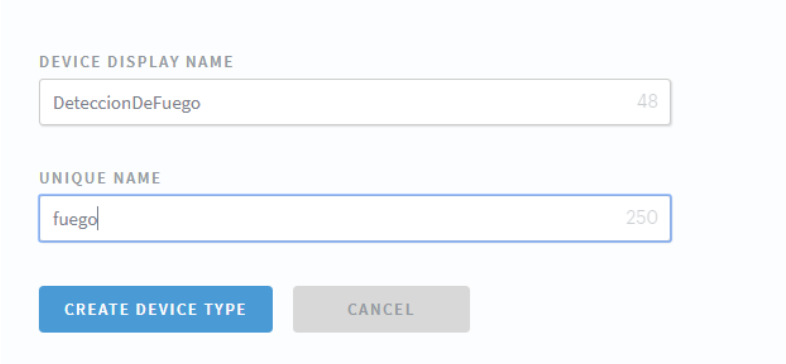
D. Luego se debe dar clic en Divice Types



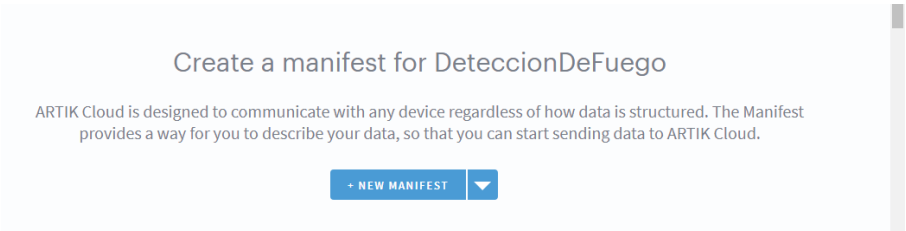
E. Se da clic en + New Divice Type



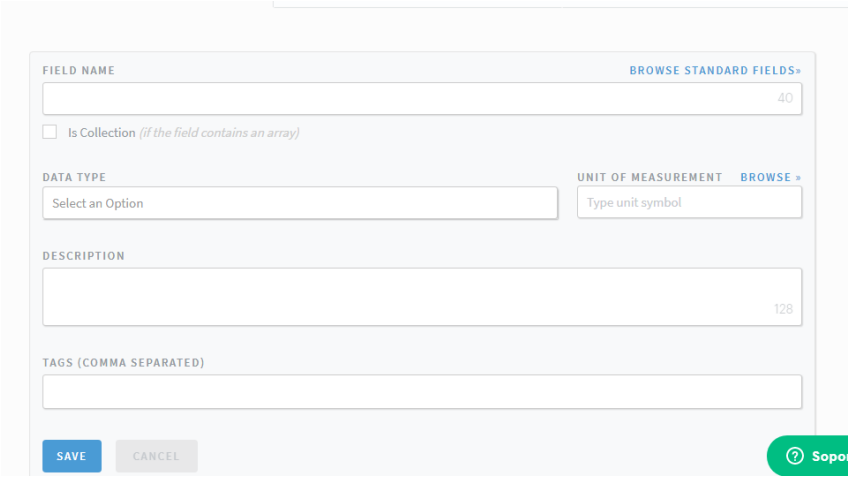
F. Luego llenamos los siguientes campos y damos clic en Create Device Type.



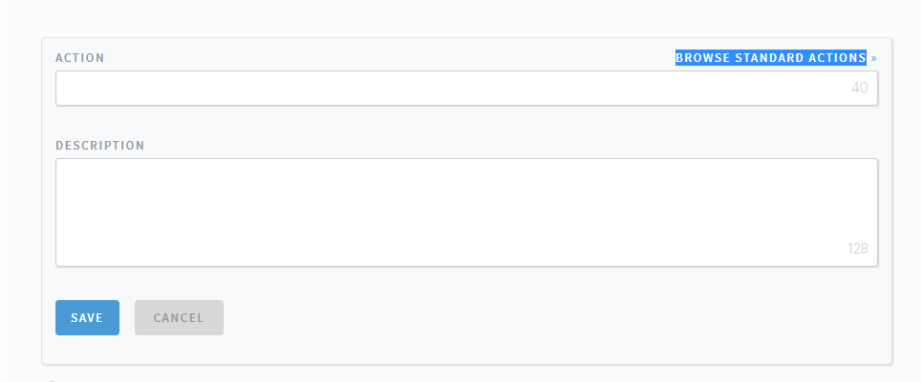
G. Posteriormente, se pasa a crear un manifiesto, dando clic en New Manifest



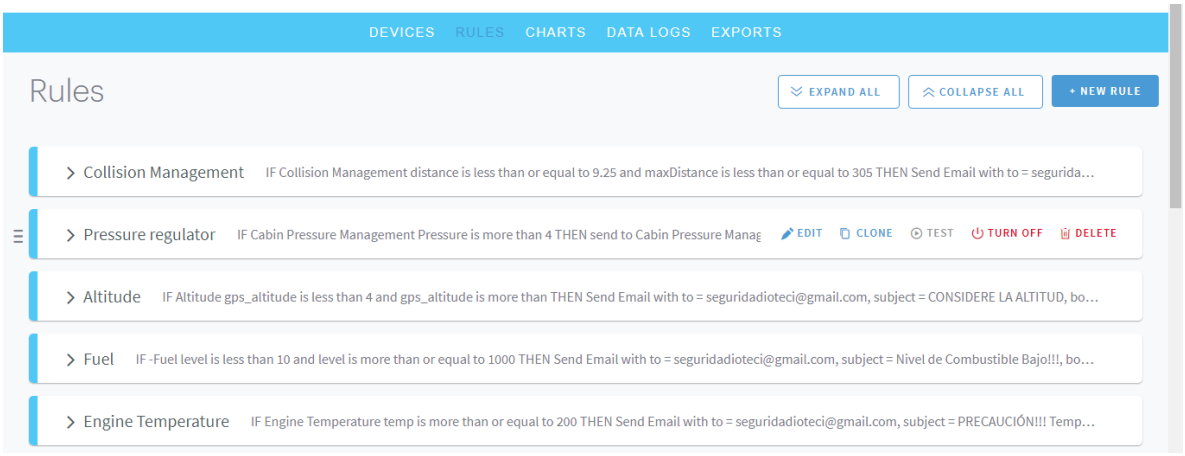
H. Ahora, se deben llenar los siguientes campos y se debe dar clic en Save:



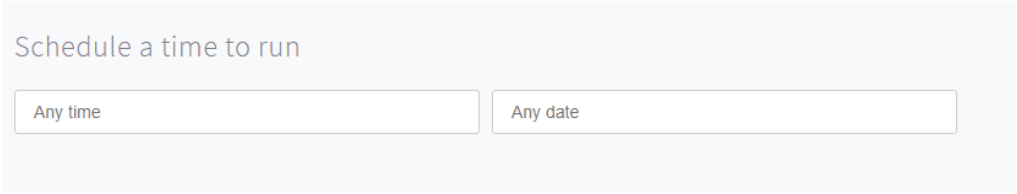
I. Haga clic en la pestaña Device Actions para añadir opcionalmente Acciones que el tipo de dispositivo puede recibir. Al igual que con los campos del dispositivo, el formulario sugiere automáticamente las acciones estándar. Para ello, puede hacer clic en BROWSE STANDARD ACTIONS ver las acciones que ya están disponibles. Finalmente se da clic en Save.



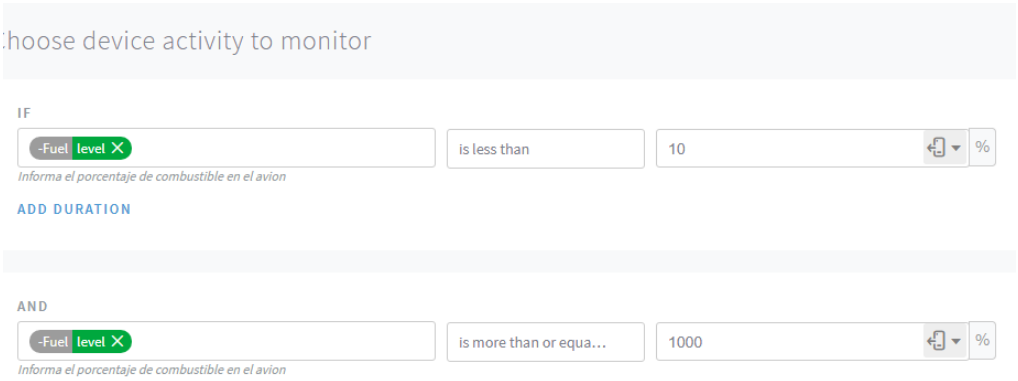
J. Finalmente se da clic en Activate Manifest.
K. Samsung Artik, permite la creación de reglas, para que ayuden a determinar cuándo un dispositivo, sufre un comportamiento extraño o reporta alguna anomalía. Para ello damos clic en Rules y luego Clic en New Rule.



L. Se define que la regla funcionara en todo momento

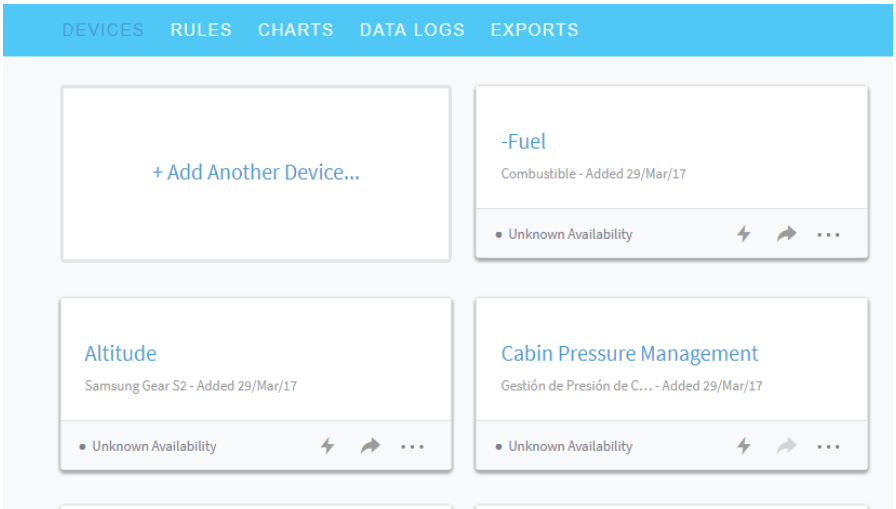


M. Ahora se define, el comportamiento lógico de la regla. Para ello, se puede establecer el dispositivo a tratar, en este caso Fuel. Determinar si la regla se active cuando el sensor detecta un valor mayor, mayor igual, menor, menor igual, igual, entre otras operaciones.



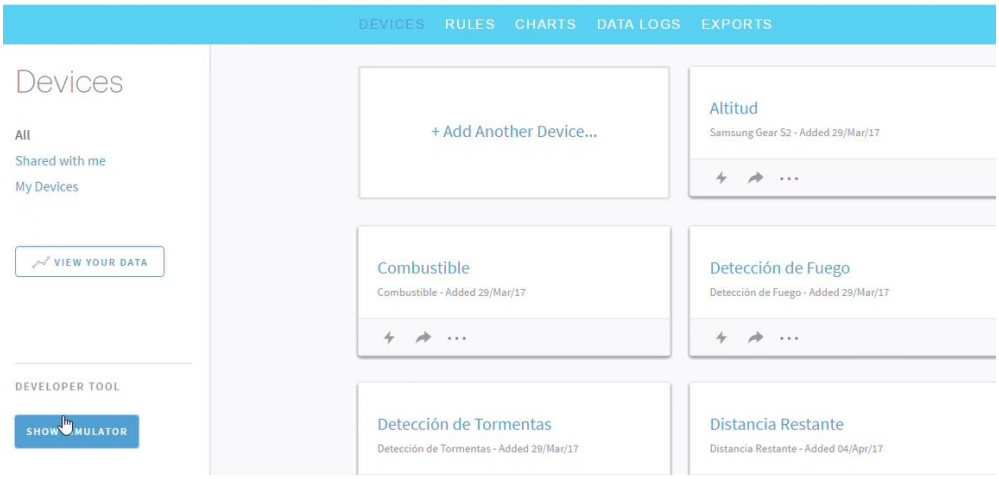
N. Posteriormente, se agrega una alerta, determinando un correo electrónico al cual llegara dicha alerta y el mensaje que contendrá esta alerta. Finalmente se da clic en Save Rule.

O. Lo que resta, es llevar a cabo la simulación del dispositivo, para ellos se da clic en Devices:

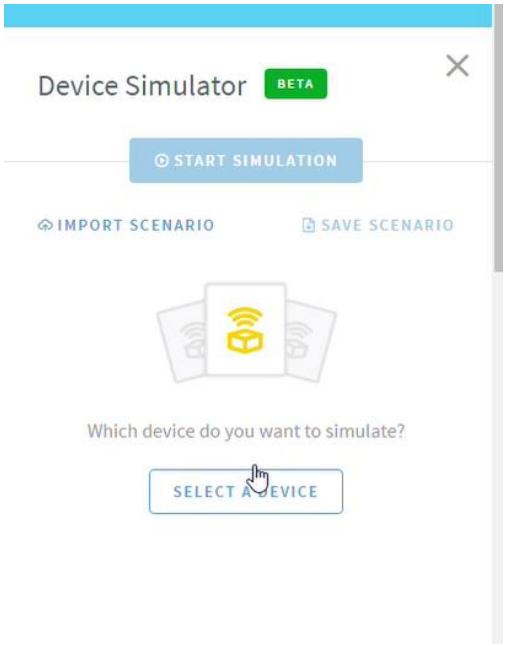


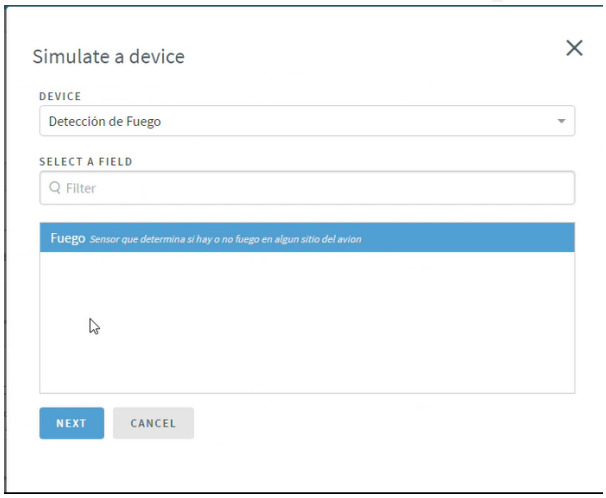
En esta sección, aparecen los dispositivos que el usuario a creado.

P. Se debe dar clic en Show Simulator



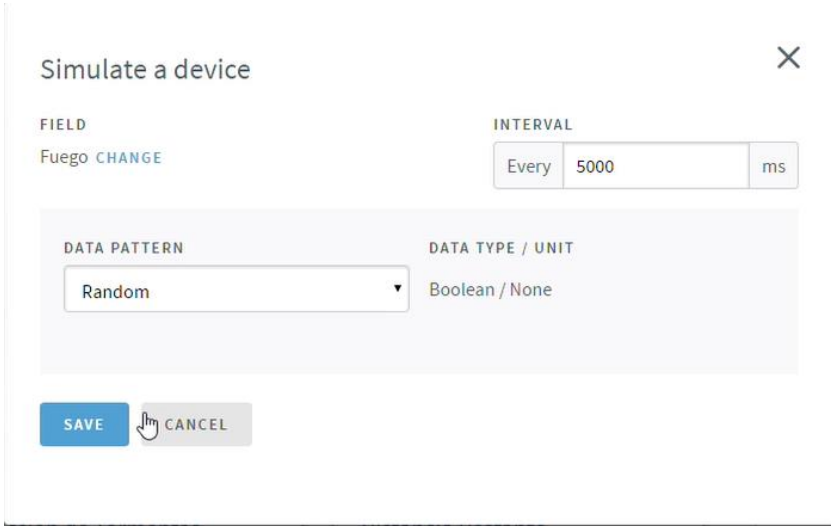
Q. Luego se selecciona el dispositivo:



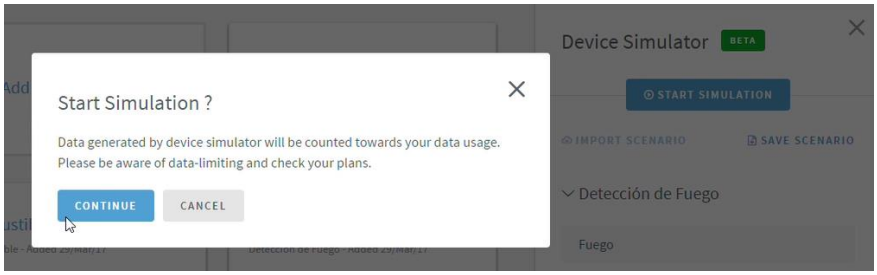


Ahora se da clic en next.

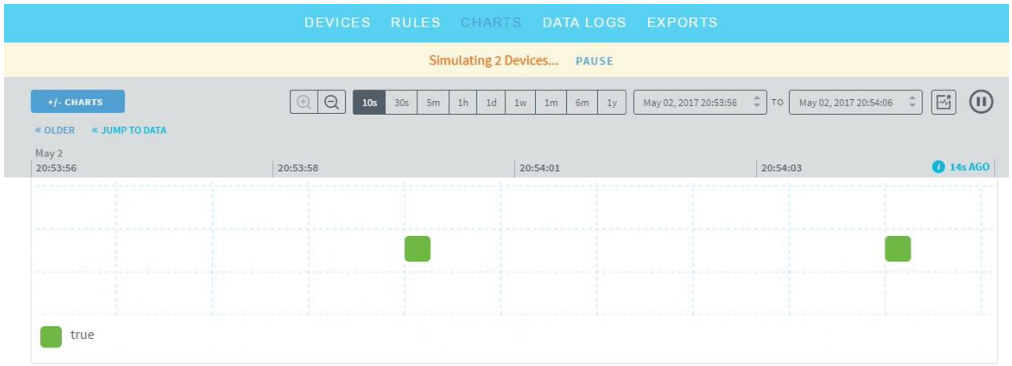
R. Se determina el comportamiento del dispositivo y se da clic en Save



S. Se da clic en Start Simulation y luego en Continue



T. Finalmente, en la pestaña Charts, se verá el comportamiento del dispositivo:



Aparte de estas implementaciones, como ya se ha mencionado en otros apartes del libro, el proyecto de grado, tanto PGR1, como PGR2, nos permitieron llevar a cabo la entrega de dos productos de alta importancia, como lo son la elaboración de dos artículos, el primero llamado ***Hacia la Seguridad de IoT: Revisión de Escenarios*** y está orientado hacia el

ámbito de investigación**.** El segundo, se realizó como trabajo correspondiente a PGR2, este artículo tiene por nombre ***Reporte de Caso: Implementación de Servicios IoT Seguros,*** y como su nombre lo indica, es un artículo que está orientado a un reporte de caso, en cuanto a la experiencia obtenida en PGR2.

En la actualidad, estos dos artículos están teniendo un proceso de revisión, por diferentes personas, conocedoras del tema de Internet de las cosas y se pretende que al estar complemente listos, estos artículos sean sometidos a publicación en revistas internacionales o bien, hagan parte de conferencias referentes a los temas tratados.

8. SOFTWARE MANEJADO

A. Packet Tracer

B. VirtualBox

C. OpenIoT

D. Linux

E. Samsung Artik

F. IBM Watson IoT

G. Windows 10

H. Node Red

9. CONCLUSIONES

Internet de las Cosas, es un concepto que actualmente está en auge, lo cual trae consigo diversas oportunidades dentro de este campo, ya sea de investigación y/o desarrollo, lo cual se buscó en este proyecto, lo cual se logró, ya que se hizo un trabajo de investigación bastante amplio y también se logró desarrollar un poco, un producto orientado a este ámbito.

Pero realizando un enfoque, en lo que compete en este proyecto, como lo es la seguridad orientada a internet de las cosas, se puede ver que es un tema que aún es algo joven en cuanto a implementación. Es joven en cuanto a implementación, porque en teoría se encuentra en diferentes sitios, como se tiene conciencia de la importancia de la seguridad en este tema, pero llevando a cabo una revisión de algunas de las tantas plataformas IoT, que hay en el mercado, es decir, pasando ahora a la práctica, no es tan claro como lleva a cabo la implementación del aspecto de seguridad en cada una de estas plataformas IoT. Pero es importante dejar claro, que, aunque no se tenga

claridad de la implementación de este aspecto, no quiere decir que las plataformas IoT no lo estén desarrollando, sino que apenas está en un nivel de desarrollo joven. (Tomado del articulo realizado en proyecto de grado 2)

BIBLIOGRAFÍA

- L. Atzori, A. Iera y G. Morabito, «The Internet of Things: A survey,» de Computer Networks, Italia, 2010, pp. 1-3.
- Wikipedia. Internet de las Cosas. Disponible en Internet: https://es.wikipedia.org/wiki/Internet_de_las_cosas
- Bussines Value Exchange. Seguridad en Internet de las Cosas: Los nuevos desafíos. Disponible en Internet: https://businessvalueexchange.com/es/2015/05/27/seguridad-en-internet-de-las-cosas-los-nuevos-desafios/
- Hackster.io. Connecting Hexiwear with ARTIK Cloud using Device Simulator. Disponible en Internet: https://www.hackster.io/wesee/connecting-hexiwear-with-artik-cloud-using-device-simulator-ec1f0c
- Revista Semana. Tragedia en Antioquia: 71 muertos deja accidente de avión en el que viajaba equipo Chapecoense. Disponible en Internet: http://www.semana.com/nacion/articulo/se-estrella-avion-de-chapeconse-en-antioquia/507230