|  |  |
| --- | --- |
| **Descripción: C:\Users\Oswaldo Castillo\Documents\Oswaldo Castillo Navetty\Institucional\Logotipo Programa Sistemas.jpg** |  |

1. **Información general del proyecto de grado**

|  |  |
| --- | --- |
| Nombre | DEVELOPMENT OF IOT DEVICES |
| Director | DANIEL ORLANDO DÍAZ LOPEZ |
| Equipo de estudiantes | MANUEL FELIPE SANCHEZ RIAÑO |
| Grupo de investigación | Ciencia, Tecnología y Gestión - CTG-Informática |
| Línea de investigación | Informática y Domótica |
| Proyecto de investigación al que pertenece | Información que deberá ser suministrada por el director de proyecto |
| Duración (meses) | 9 |

1. **Resumen ejecutivo**

Actualmente estamos atravesando la era de la revolución tecnológica, donde dia a dia se avanza casi de manera exponencial, a tal punto de llegar a pensar en como crear una autonomía en las cosas que nos rodean.“Inthernet of Things” es un concepto que se basa en la interconexión de objetos de la vida diaria con internet creando a su vez un medio para comunicarse con el mismo de manera interactiva. El presente proyecto esta orientado al desarrollo e implementación de dispositivos IoT por medio de una combinación de diferentes hardware y software que permitan diferentes funcionalidades en objetos de uso diario así como visualizar los impactos a nivel de seguridad en la creación y puesta en funcionamiento de estos dispositivos.

1. **Descripción del proyecto**
   1. **Planteamiento del problema.**

El desarrollo de Dispositivos IoT es básicamente la conexión a través de internet de una gran cantidad de objetos o dispositivos, en este aspecto la implementación de estos dispositivos ha venido evolucionando en los últimos años siendo usados en escenarios como domótica,, manufactura, el sector industrial entre otros. Actualmente estos dispositivos son realmente atractivos para algún ciber-atacante pues las inversiones en seguridad para estos dispositivos aún no son suficientes y no se garantiza un nivel idóneo de protección en los mismos. Cada dia se crean mas dispositivos IoT su volumen de crecimiento es realmente alto es por esto que cualquier ataque podría implicar un impacto significativo desde una fuga de información, una denegación del servicio e incluso también una alteración peligrosa de un proceso definido. En el presente proyecto nos vamos a enfocar a analizar y evaluar estas brechas de seguridad para después enfocarse en crear dispositivos que aseguren un alto nivel de confiabilidad y seguridad en la información que transmiten o reciben.

* 1. **Justificación.**

Los dispositivos de internet de las cosas son cada vez más comunes (televisores, teléfonos, bicicletas, equipos de medición ambiental o médica, etc.), y su uso extensivo hace que estos sean un elemento de ataque muy atractivo para diferentes tipos de adversarios. Según Gartner, en el 2016 las inversiones realizadas en seguridad IoT fueron de 348 millones de dólares, estimando que para el año 2016 habran más de 6.000 millones de dispositivos IoT y para el 2020 más de 20.000 millones en todo el mundo. Al ser usados los dispositivos IoT en escenarios como domótica, manufactura, gestión ambiental, salud, entre muchos otros, se puede vislumbrar el gran impacto que podría causar una afectación de seguridad sobre estos elementos. Los impactos podrían ir desde fuga de información sensible que sea almacenada en dispositivos IoT, hasta una alteración peligrosa de procesos industriales causando incluso afectaciones a la integridad humano además de impactos económicos. Debido a la gran diversidad existente en los dispositivos IoT, principalmente por la diversidad de funcionalidades incorporadas, la gran oferta de fabricantes y los diferentes tipos de arquitecturas, se pone de manifiesto que el aseguramiento de estos dispositivos es un reto real que se hace necesario afrontar de forma urgente.

* 1. **Objetivos Generales:**
* Desarrollar competencias en el diseño y construcción de dispositivos IoT con capacidades de sensorización y actuación.
* Realizar un análisis en términos de seguridad para dispositivos IoT con capacidades de sensorización y actuación.
  1. **Objetivos Específicos**:
* Identificar los métodos existentes para el diseño, simulación y construcción de dispositivos IoT, preferiblemente de tipo open source.
* Realizar el diseño de un dispositivo IoT con aplicación a un escenario IoT de domótica.
* Implementar el dispositivo IoT de acuerdo a las funcionalidades definidas previamente.
* Realizar pruebas de operación del dispositivo IoT en un escenario IoT.
* Evaluar la seguridad del dispositivo IoT implementado.
  1. **Alcance del proyecto**:

Se realizara la implementación de 4 dispositivos IoT que tengan capacidades de sensorización y actuación con el uso de a lo sumo dos soluciones de hardware y software dife. Se establecerá para cada dispositivo un paquete de pruebas para evaluar la funcionalidad y seguridad de cada prototipo y también, Se realizara el manual de configuración e implementación de los mismos. El tiempo estimado para el desarrollo de del proyecto es de 6 meses.

* 1. **Metodología propuesta**:

Para la implementación de los dispositivos IoT se debe realizar una validación en términos de viabilidad, costos y tiempo sobre cada uno de los dispositivos elegidos para implementar.Posteriormnente se procederá con la simulación de cada dispositivo IoT haciendo uso de maquinas virtuales para emular el S.O en el cual se implementaran los mismos. Luego de esto se procederá a la realización del dispositivo con la configuración en el hardware y el software que se ha definido y emulado previamente. Con el dispositivo implementado el siguiente paso será realizar el conjunto de pruebas validando el funcionamiento de las operaciones que deberían realizar los mismos y luego de realizar dichas pruebas se realizar una evaluación en términos de seguridad de cada uno de los dispositivos todo esto se espera implementar en un escenario de Domotica IoT.

* 1. **Área de aplicación del producto resultado del proyecto**:

Los dispositivos IoT tienen la capacidad de capturar y analizar datos generados por varias fuentes de medición y a su vez procesarlos en tiempo real Esta tecnología puede ayudar a las pequeñas y medianas empresas que quieran tener una visión en tiempo real de lo que esta pasando en su negocio y al mismo tiempo puedan tomar decisiones de manera instantánea, en el presente proyecto se realizara la aplicación de estos dispositivos en un escenario de Dómotica donde un conjunto de sistemas y tecnologías permitirán la automatización de algunos objetos de uso cotidiano en una casa, una oficina etc.

* 1. **Resultados esperados**:
* **Diseño e implementacion de dispositivos iot**
* **manual de configuración e implementación de los prototipos**
* **plan de pruebas de funcionalidad y seguridad diseñado**
* **resultado de plan de pruebas**
* **propuesta de mejora a soluciones evaluadas**
  1. **Usuarios potenciales directos e indirectos de los resultados de la investigación**

Este proyecto va dirigido principalmente a las Fuerzas Militares (FFMM) y a la Unión Europea, pero también a cualquier persona natural o jurídica que tenga conocimiento sobre “Internet of Things” y quiera conocer los diferentes aspectos involucrados en la implementación de dispositivos IoT tanto en términos de viabilidad, costo y tiempo como también en un aspecto muy relevante que es la seguridad dado que actualmente los usuarios que realizan alguna implementación IoT muchas veces no se preocupan por este aspecto siendo que es quizá el mas importante cuando estamos accediendo a internet en este caso para dar ordenes o recibir información precisa de algún objeto que ahora llamaremos “dispositivo inteligente” pues tendrá la capacidad de comunicarse con el usuario a través de internet respondiendo a numerosas peticiones en cualquier momento. Es por esto que se espera tener un nivel de seguridad idóneo para evitar a toda costa la manipulación de estos dispositivos por personas externas que puedan el funcionamiento y confiabilidad del mismo.

* 1. **Herramientas de software utilizadas**

Para la implementación de los dispositivos IoT se hará uso de varios componentes de software en principio se utilizara Virtual-Box para el montaje y emulación, se hará uso de la librería WebIOPI para la conexión y control de los sensores y actuadores que posea el dispositivo por medio de internet esta configuración se realizara en un S.O Raspbian. Para otros dispositivo se utilizara el S.O Microsoft Windows 10 IoT junto con Microsoft Azure para enviar los datos que reciba a través de internet. También se hara uso de AndroidStudio para realizar un control del dispositivo por medio de un dispositivo móvil. Se realizaran algunos Scripts en Python que se encargaran de ejecutar una función determinada sobre un dispositivo. Se espera tener un repositorio en una plataforma como GitHub o BitBucket para el seguimiento y control de versiones en cuanto se va avanzando en el proyecto.

* 1. **Posibles publicaciones o conferencias donde someter el articulo generado en PGR2:**
* Revista de la Escuela Colombiana de Ingeniería , *Desarrollo de un escenario IoT con un enfoque en seguridad basado en Seguridad en el Dispositivo, Seguridad en la Nube y la Gestión del ciclo de vida de la seguridad- Bogotá D.C, Colombia*.
* Barcamp Security Edition 2018, *Diseño e implementación de Dispositivos IoT con un enfoque en los tres pilares de seguridad- Bogotá D.C,Colombia*.
* Foro en Seguridad de la Información.Seguridad en IoT, una tecnología emergente en la era de la economía digital, Universidad de los Andes - Bogotá DC, Colombia:

El foro está dirigido a profesionales interesados en las oportunidades que emergen para responder a las necesidades de seguridad en el contexto de Internet de las cosas.

.

* 1. **Logros:**
* Se logra la implementación de 3 dispositivos IoT realizando una identificación previa de los métodos utilizados en la creación de los mismos, permitiendo la puesta en marcha de un escenario de domótica (Smart Home) con la veracidad de que cada dispositivo tiene tanto una arquitectura como un sistema operativo diferente .
* Se realizan pruebas de operación para el conjunto de dispositivos implementados, donde se pudo evidenciar para cada dispositivo como se encarga de enviar o recibir peticiones de la nube para realizar una determinada acción.En el caso del OSMC se realizó la configuración de internet en el dispositivo para la posterior instalación de diferentes addons y repositorios, se revisa la funcionalidad y el contenido de cada addon instalado.
* Se realiza un análisis de seguridad para el escenario de dispositivos IoT implementado haciendo uso de diferentes herramientas para explotar las vulnerabilidades que se encontraron en los dispositivos.Evidenciando las posibles brechas de seguridad que puede tener un escenario IoT y las repercusiones o consecuencias que puede traer la explotación de las mismas.
  1. **Bibliografía**:
* Anon, (2017). [online] Available at: http://www.shahrvan.org/wp-content/uploads/2016/06/Designing-The-Internet-Of-Things.pdf [Accessed 10 Sep. 2017].
* SAP. (2017). *¿Qué es internet de las cosas? | Tecnología de IoT | SAP*. [online] Available at: https://www.sap.com/latinamerica/trends/internet-of-things.html [Accessed 10 Sep. 2017].
* ENTER.CO. (2017). *Citar un sitio web - Cite This For Me*. [online] Available at: http://www.enter.co/especiales/colombia-conectada/iot-les-permite-a-las-pymes-tener-visibilidad-y-control-de-su-negocio/ [Accessed 10 Sep. 2017].
* Webiopi.trouch.com. (2017). *Tutorial : Using devices*. [online] Available at: http://webiopi.trouch.com/Tutorial\_Devices.html [Accessed 10 Sep. 2017].
* Gemalto.com. (2017). Asegurando el Internet de las Cosas. [online] Available at: https://www.gemalto.com/latam/iot/seguridad-en-iot [Accessed 4 Dec. 2017].
* BBVAOpen4U. (2017). Cuando el IoT no es el Internet de las cosas, sino la Identidad de las cosas. [online] Available at: https://bbvaopen4u.com/es/actualidad/cuando-el-iot-no-es-el-internet-de-las-cosas-sino-la-identidad-de-las-cosas [Accessed 4 Dec. 2017].