ARQUITECTURAS DE REFERENCIA PARA IOT CON TRANSFERENCIA SEGURA DE INFORMACIÓN

ANDRÉS VÉLEZ PÉREZ
INGENIERO DE SISTEMAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA

ESPECIALIZACIÓN DE SEGURIDAD INFORMÁTICA

TULUA

2019

ARQUITECTURAS DE REFERENCIA PARA IOT CON TRANSFERENCIA SEGURA DE INFORMACIÓN

ANDRÉS VÉLEZ PÉREZ
INGENIERO DE SISTEMAS

MONOGRAFÍA

DIRECTOR MARTIN CAMILO CANCELADO RUIZ
ESP. SEGURIDAD INFORMÁTICA

DOCENTE CHRISTIAN REYNALDO ANGULO RIVERA
MBA, ESP. SEGURIDAD INFORMÁTICA
PROYECTO DE SEGURIDAD INFORMÁTICA II

DOCENTE LUIS FERNANDO ZAMBRANO
PROYECTO DE SEGURIDAD INFORMÁTICA I

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA

ESPECIALIZACIÓN DE SEGURIDAD INFORMÁTICA

TULUA

2019

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del Jurado

_____
Firma del jurado

_____
Firma del jurado

Tuluá, 21 abril de 2019.

Para todas aquellas personas que sufren por la ley de Murphy, «Anything that can go wrong will go wrong».

Gracias a Dios por darnos destreza e inteligencia. A nuestras familias que con su apoyo y compresión supieron entender los momentos difíciles de nuestra carrera y a todas aquellas personas que de una u otra manera contribuyeron a que se logrará culminar con éxito esta etapa de nuestra vida.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE FORMULAS

LISTA DE ANEXOS

GLOSARIO

ARM: es una arquitectura RISC (Reduced Instruction Set Computer – Conjunto reducido de instrucciones).

BROKER: es un programa que actúa como un intermediario entre dos sistemas, como un sistema de mensajería.

COSA: se define como un dispositivo electrónico con capacidades de procesamiento.

ENCRIPTACION: cifrar datos usando algún algoritmo que permite ocultar información en forma no comprensible que puede ser descifrado con la misma clave.

GATEWAYS: dispositivo que actúa como interfaz de conexión entre aparatos y dispositivos.

IOT: Internet of Things, Internet de las cosas o de los objetos.

MEDIACION: desarrollo de software a la medida que sirve para enlazar dos sistemas.

RESUMEN

La seguridad sobre IoT (Internet of Things, en español, Internet de las cosas o de los objetos) es un aspecto muy importante en este mundo conectado, los diseños (arquitecturas) para transferir información de forma segura se han vuelto críticos, no solo basta con conectar un sensor y que trasmita datos, hay que tener en cuenta la seguridad en todos sus aspectos, ya que la integralidad de estos supone que su proceso se esté llevando a cabo de forma adecuada.

De tal forma es importante describir los posibles riesgos que involucran esta clase de tecnología y como se puede mitigar para el buen funcionamiento de IoT, con el fin que diferentes dispositivos (microcontroladores con conectividad inalámbrica, mini-ordenadores ARM) se integren de manera eficiente y segura, se debe definir las bases y lineamientos para la trasferencia segura de información. Con tal fin se describen las diferentes arquitecturas propuestas por organismos de estandarización y autores que proponen otros diseños con un principio transversal que es la seguridad.

INTRODUCCIÓN

Este trabajo monográfico presenta los modelos y arquitecturas/modelos de IoT usadas, describiendo los diferentes componentes que los integran y las tecnologías asociadas al internet de las cosas.

El Internet de las Cosas, consiste en una red interconectada de dispositivos (cosas u objetos), que son sensores que tiene la capacidad de generar y transmitir información hacia la nube (internet) o servidor, esta información que es transmitida puede estar expuesta a riesgos que degradan la información con consecuencias inesperadas para los servicios que estos están monitoreando.

El IoT tiene muchos usos potenciales (hogar, fábricas, oficinas, centros de salud, etc.)[1], el cual hace que exista una gran variedad de dispositivos (cosas) que de alguna forma están transmitiendo información que puede verse afectada por entes externos y que no tienen un diseño (arquitectura) que permita reducir estos riegos.

[1] COMPUTEX TAIPEI, Internet of Things Ecosystem, 2014.

DEFINICIÓN DEL PROBLEMA

El Internet de las Cosas (IoT, del inglés Internet of Things), consiste en una red interconectada de dispositivos (cosas u objetos), que son sensores, los cuales tienen la capacidad de generar y transmitir información hacia la nube (internet) o servidor, esta información que es transmitida puede estar expuesta a riesgos que degradan la información con consecuencias inesperadas para los servicios que estos están monitoreando.

En este sentido se ha vuelto critico la seguridad de la data transmitida por estos dispositivos ya que transfieren la información de forma inalámbrica (WiFi, Bluetooh, 3G, 4G), algunos dispositivos no tienen la suficiente capacidad de procesamiento para generar canales seguros (encriptación de datos) entre el dispositivo inicial y su destino final, es por esto que se busca los mejores estándares/modelos con el fin de divulgar y cerrar la brecha de conocimiento ya que se esperan 500 billones de dispositivos para el 2030[2], en el 2017 fueron 17 billones, y los riesgos de dispositivos comprometidos se cuentan por millares[3]. En Colombia el proveedor Telefónica tiene un total 600.000 soluciones IoT con 14.000 clientes[4], el cual corresponde al 60% del mercado empresarial, es decir, que en Colombia supera el millón de dispositivos IoT conectados.

[2] CISCO, Cisco Visual Networking Index: Forecast and Trends, 2017-2022.
[3] En el 2017 un malware denominado BrickerBot destruyo de forma permanente más 10 millones de dispositivos IoT, ÁLVAREZ R., 2019, Revista digital Xataka.
[4] TELFONICA, 2108

JUSTIFICACION

El IoT tiene muchos usos potenciales (hogar, fábricas, oficinas, centros de salud, etc.)[5], el cual hace que exista una gran variedad de dispositivos (cosas) que de alguna forma están transmitiendo información que puede verse afectada por entes externos y que no tienen un diseño (arquitectura) que permita reducir estos riegos de acuerdo a la capacidad del dispositivo, cada tipo de dispositivo puede tener una forma segura de transmitir información, con el fin de mitigar al máximo los riesgos al cual están expuestos.

En el mercado cuenta con dispositivos con conectividad WiFi con pocos recursos de hardware como ESP8266[6] (Arduino compatible) y su incapacidad de generar cifrados seguros a comparación de dispositivo ARM como un Raspberry Pi[7] el cual tiene un Sistema operativo; y no es microcontrolador programado con bajos recursos, estas diferencias hacen que la arquitectura a ser usada pueda integrar cualquier clase de dispositivo IoT. Un ejemplo puede ser que el microcontrolador no exponga directamente, sino que pasen por un bróker (mediación) que entregue o agregue la capa de seguridad que permita su exposición segura hacia el internet.

Esta exposición insegura tiene implicaciones sociales haciendo vulnerable las empresas y los individuos que usan este tipo de tecnología, el uso de conexiones inseguras causa perdida de información y desconfianza es por esto por lo que se busca los mejores estándares en el mercado con el fin de recopilar las mejores arquitecturas/modelos y tener el conocimiento necesario para diseñar conexiones entre dispositivos IoT de forma más segura con estándares de calidad.

[5] COMPUTEX TAIPEI, Internet of Things Ecosystem, 2014.
[6] ESPRESSIF, Esp8266 Arduino Compatible, 2017.
[7] RASPBERRY PI, 2017.

OBJETIVOS GENERAL Y ESPECIFICOS

OBJETIVO GENERAL

Realizar un estudio monográfico del diseño (arquitectura) u transferencia de información segura en IoT, mediante el análisis de las diferentes propuestas que existen para la transferencia de datos con enfoque en la capa uno.

OBJETIVOS ESPECÍFICOS

1. Analizar los principales estándares en arquitecturas de las redes IoT.
2. Describir los riesgos a los cuales está expuesto la transferencia de información de los dispositivos IoT con conectividad WiFi en la capa uno.
3. Analizar los métodos seguros actuales de transferencia de Información en IoT.
4. Proponer el diseño (arquitectura) transferencia segura de información en IoT en la capa uno.

MARCO CONCEPTUAL Y TEÓRICO

El termino Internet de las Cosas (Internet of Things, abreviado IoT) es un término acuñado por Kevin Ashtom en 1999[8] que nació bajo el nombre de una presentación de RFID; En 2005, la Unión Internacional de Telecomunicaciones publicó una investigación sobre Internet of Things, definiéndola como "incorporación de transceptores móviles de corto alcance en una amplia gama de dispositivos adicionales y artículos de uso diario, permitiendo nuevas formas de comunicación entre personas y cosas, y entre las cosas mismas."[9], Pero en la recomendación ITU-T Y-2060 su definición es "infraestructura global de la sociedad de la información, que permite ofrecer servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperatividad de tecnologías de la información y la comunicación (TIC) presentes y futuras"[10], este último concepto es aplicable a la siguiente formula[11]:

Fórmula 1 IoT Formula

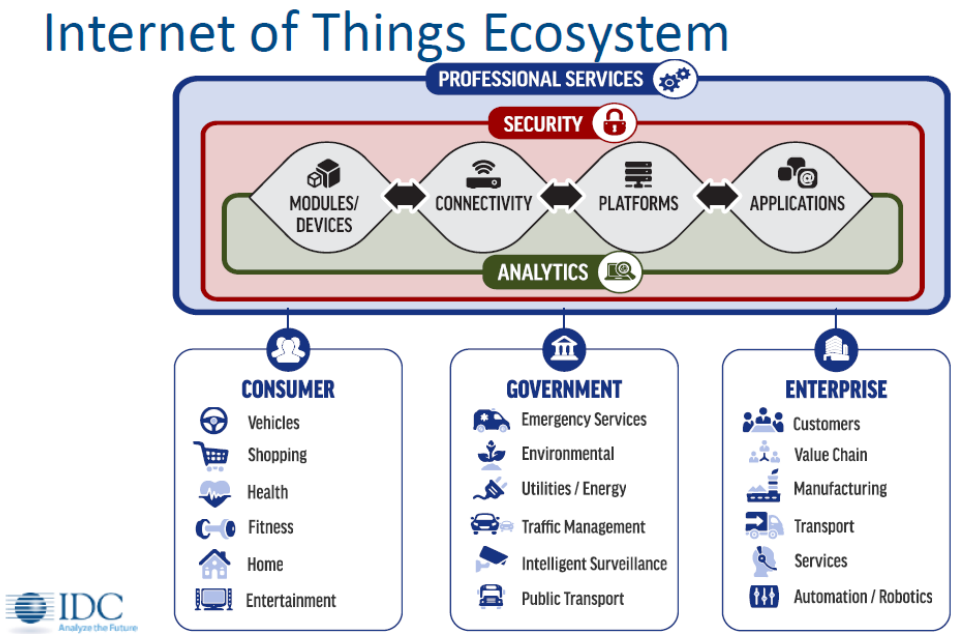
Objeto Físico + (Controlador + sensor + actuador) + Internet = IoT

McEwen & Cassimally, Designing the Internet of Things, 2013.

Esta fórmula brinda la base de ecosistema en el cual puede interactuar una gran variada de sectores. En la Figura 1, muestra un ecosistema completo de IoT[12]:

[8] Primer uso dado al termino Internet of Things, ASHTON, That 'Internet of Things' Thing, 2009.
[9] Definición de IoT citado por: Lee, 2017.
[10] International Telecommunication Union, Definición en de IoT en la recomendación ITU-T Y-2060, 2012.
[11] Fórmula para determinar un dispositivo IoT: McEwen & Cassimally, Designing the Internet of Things, 2013.
[12] La figura se encuentra disponible en la presentación de COMPUTEX TAIPEI y el autor del libro de Geng, 2017 la usa en la «Figura 1.5».

Figura 1 IoT Ecosystem



Presentación de COMPUTEX TAIPEI.

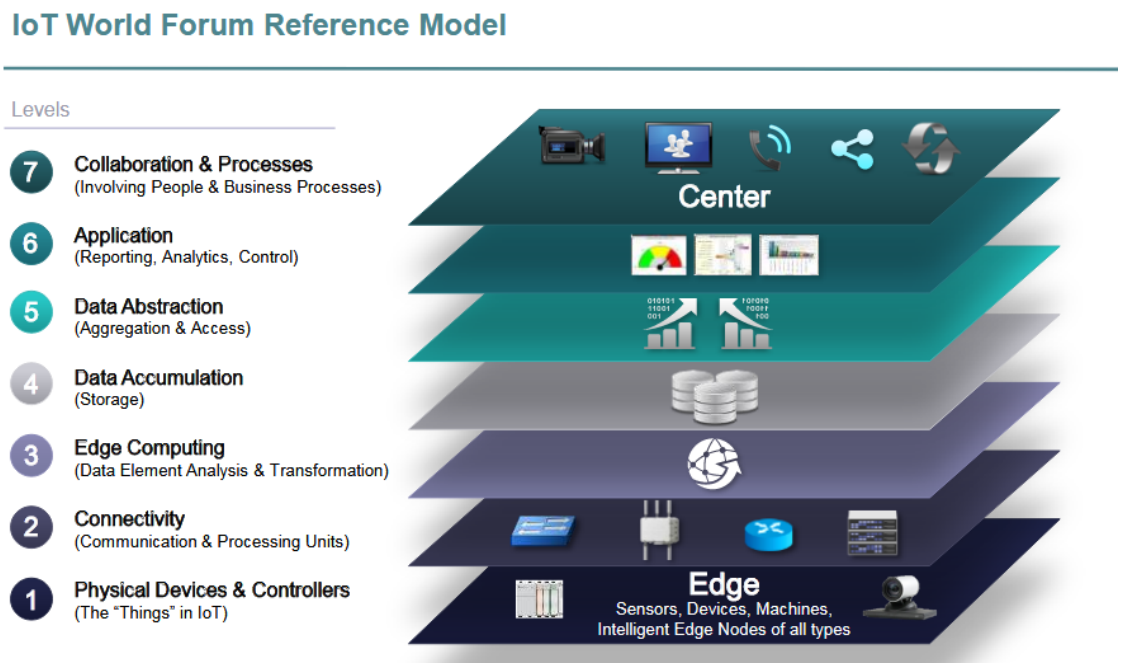
Este ecosistema muestra la interacción de consumidores, gobierno y empresas, en las cuales pueden ver un valor agregado en el uso de IoT, en la cual podemos encontrar:

- Personas del Común (Consumidor)
    - Hogar conectado, cámara de vigilancia, sensores en la puertas y ventanas, electrodomésticos conectados.
    - Vehículo inteligente.
    - Pulseras para el ejercicio.
    - Sistemas de entretenimiento.
- Empresas del Gobierno
    - Trafico inteligente, control de semáforos, cámaras.
    - Servicios públicos.
    - Cálida de vida, control de ambiental (calidad del aire)
- Empresas

- Fábricas, automatizando procesos.
- Hospitales, clínicas en el cuidado del paciente.
- Logística, entrega de paquetes (rastreo).
- Manufacturación, sensores, robots, software.

Este ecosistema trabaja bajo la funcionalidad de los dispositivos que proporcionan toda la información que se necesita de acuerdo con su utilidad, pero todo este esquema depende una modelo de arquitectura funcional, la IoT World Forum propone un modelo en el cual propone siete capas desde una perspectiva técnica en la cual se observan funciones específicas con una seguridad que abarca todo el modelo[13] [14], Figura 2:

Figura 2 IoTWF Reference Model



JIM GREEN, CTO Data Virtualization, 2014, Figura 2.

En la Tabla 1 se puede observar sus funcionalidades por capas:

[13] JIM GREEN, CTO Data Virtualization, 2014, Figura 2.
[14] BARTON, Salgueiro, & Hanes, IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things, 2017, detalle Figura 2.

Tabla 1 IoTWF Reference Model

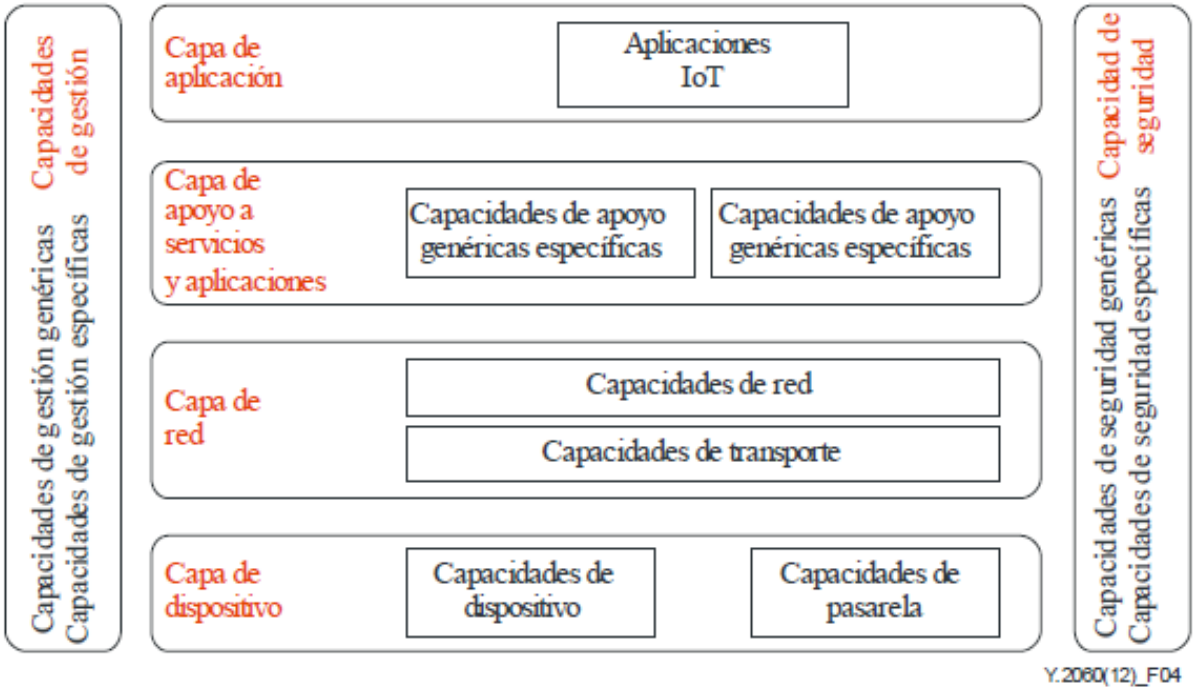
Capa	Funciones
Capa 1, Dispositivos físicos y controladores	Todos los dispositivos de diferentes tamaños lo cuales pueden enviar o recibir información.
Capa 2, Conectividad	Es la encargada de transmitir los datos en el medio deseado, swicth, router, comunicación con la capa 1.
Capa 3, Edge Computing	Transformar los datos antes de su disposición final de almacenamiento.
Capa 4, Almacenamiento de Datos	Almacenar toda la información generada.
Capa 5, Abstracción de datos	Darles forma a los datos generados
Capa 6, Aplicación	Aplicaciones para análisis de datos, reportes y monitoreo.
Capa 7, Procesos y Colaboración	Son los procesos de negocio, es decir, la interacción que se da con entre IoT personas y negocios.

IoTWF

Existen otras modelos de arquitectura con diferentes capas, el modelo recomendado por la ITU es de cinco (5) capas[15] con dos trasversales, capacidad de gestión y seguridad:

[15] Modelo de referencia recomendación ITU-T Y-2060, International Telecommunication Union, 2012.

Figura 3 Modelo de referencia ITU de IoT

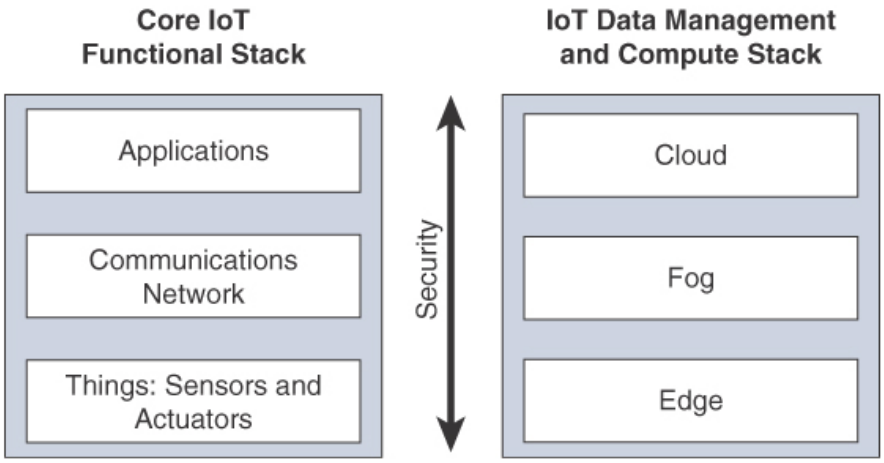


International Telecommunication Union, 2012.

Un modelo menos detallado, con una arquitectura de tres capas, se muestra en la siguiente *Figura* 4 [16], y con un stack administración de datos por capa (Edge, Fog & Cloud Computing)[17].

[16] Barton, Salgueiro, & Hanes, IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things, 2017, Cap. 3, Figura 2-6.
[17] Conceptos de del stack de la arquitectura de 3 capas Ibid.

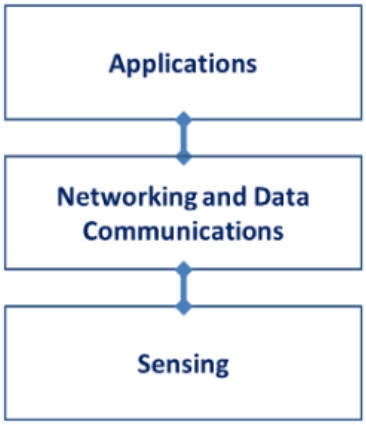
Figura 4 Arquitectura Simplificada



Barton, Salgueiro, & Hanes, IoT Fundamentals.

Un grupo de la IEEE P2413 está preparando un estándar que define un framework de arquitectura IoT[18], este grupo está proponiendo un modelo de tres capas[19] Figura 5:

Figura 5 Arquitectura de tres capas IEEE

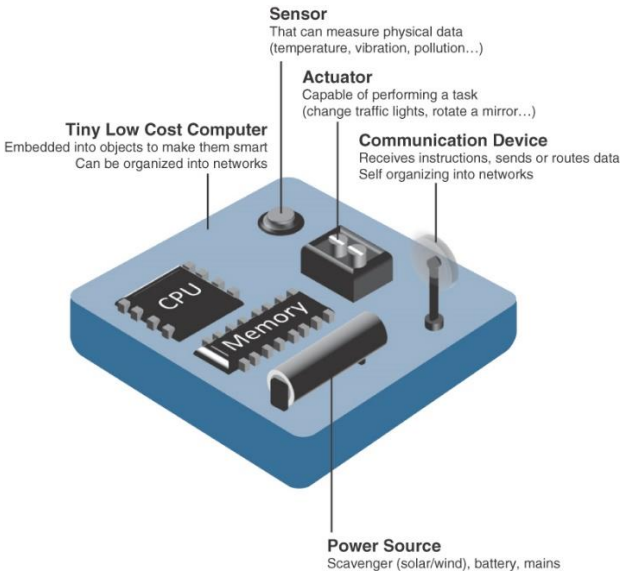


IEEE, Towards a Definition of the Internet of Things (IoT), 2015.

[18] IEEE, Internet of Things (IoT) Architecture, 2017.
[19] IEEE, Towards a Definition of the Internet of Things (IoT), 2015.

Algo en común en los modelos vistos es que el componente de seguridad es trasversal al modelo, aunque es aplicable de forma individual entre capa. Antes de continuar con la seguridad se detallará un poco la primer capa en común de los diferentes modelos, la capa uno (1) “Things” según la definición o traducción de la recomendación de la ITU (la versión en español) este es definido como un “objeto” y no su traducción literal de “cosa” se define como: “En el contexto de Internet de los objetos se trata de un objeto del mundo físico (objetos físicos) o del mundo de la información (objetos virtuales) que se puede identificar e integrar en las redes de comunicaciones.”[20], validando la definición de “objeto” encontramos que su sinónimo es “cosa”, así que su traducción es válida, en cuanto al contexto técnico, la hermenéutica[21] de que si es “cosa” u “objeto” va más de la mano en el contexto que estamos trabajando como la definición que puede tener la programación orientada a objetos[22], en el libro de Barton, Salgueiro, & Hanes[23] tratan a las “cosas” y otros nombres como una diferencia de semántica y lo definen como “Smart Objects” traduciendo esto como “Objetos Inteligentes”. Siguiendo con la definición un “Smart Objects” tiene las siguientes características (mínimas)[24] Figura 6:

Figura 6 Características de un Smart Object:



Barton, Salgueiro, & Hanes, IoT Fundamentals.

[20] El documento de recomendación tiene versión en varios idiomas, se toma la referencia del documento en español de: International Telecommunication Union, 2012.
[21] Hermenéutica: Arte de interpretar textos, originalmente textos sagrados. Definición RAE: http://dle.rae.es/?w=hermen%C3%A9utica
[22] ORACLE, What Is an Object?, 2017.
[23] BARTON, Salgueiro, & HANES, IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things, 2017.
[24] Características mínimas de un “Smart Object” de Barton, Salgueiro, & Hanes, IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things, 2017.

- Unidad de procesamiento
- Sensores y/o actuadores
- Dispositivo de comunicación
- Fuente de poder

Un ejemplo básico es un sistema de control de temperatura y húmeda[25] el cual se puede construir con:

- DHT22, el cual es el sensor de temperatura y húmeda (termómetro e higrómetro).
- ESP8266, el cual contiene unidad de procesamiento, dispositivo de comunicación que para este caso es WiFi, y una interface para conectar el sensor.
- Fuente de poder, que para este caso puede ser algún convertidor de energía (como una fuente a 5V).

Validando la Fórmula 1 y las características mínimas tenemos un objeto IoT. Este mismo ejemplo es válido cambiando el ESP8266 por un Raspberry Pi 3 (con WiFi integrado)[26].

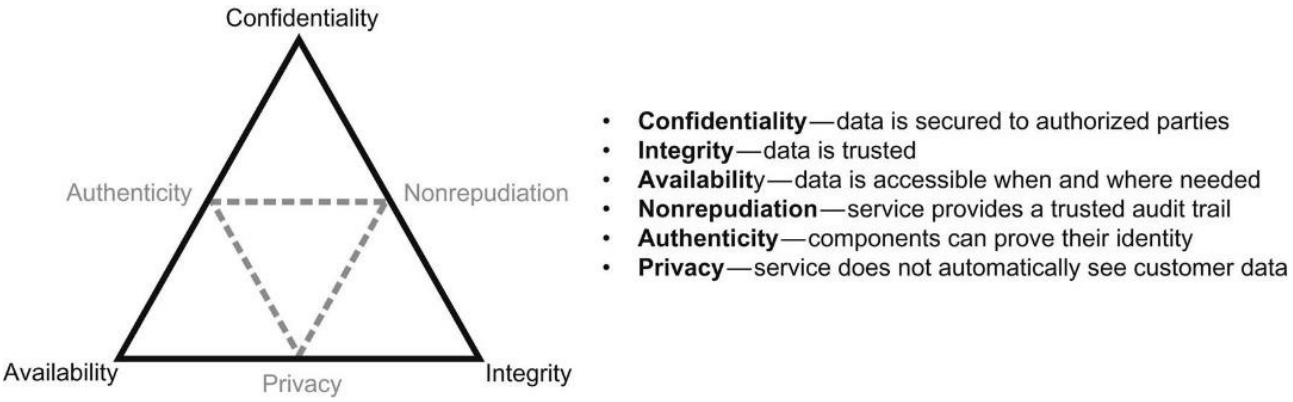
Pero con las siguientes características como objetivo para la transferencia segura de información en IoT con enfoque en la capa uno[27]:

- Autenticación
- Control de acceso
- Autorización
- Protección de la integridad.
- Validación de la integridad del dispositivo

[25] ADAFRUIT, ESP8266 Temperature / Humidity Webserve, 2015, Tutorial de temperatura y humedad.
[26] ADAFRUIT, DHT Humidity Sensing on Raspberry Pi or Beaglebone Black with GDocs Logging , 2015, Ejemplo con Raspberry pi o Beaglebone Black
[27] International Telecommunication Union, Internet of Things Global Standards Initiative, 2012, Características capa uno (1).

- Confidencialidad de datos

Figura 7 Aspectos de la Seguridad en IoT



LI DA XU & LI, Securing the Internet of Things, 2017

En la figura anterior se muestra seis aspectos de seguridad[28] para IoT.

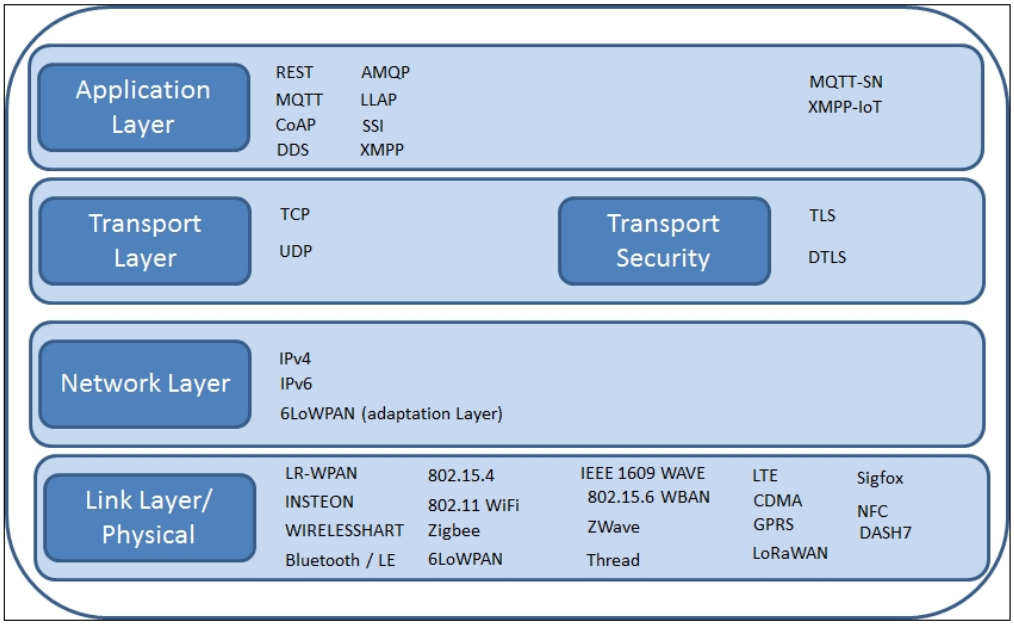
Ampliando los actores que se involucran en el ciclo de vida de IoT nos encontramos con:

- Creador del Dispositivo IoT
    - Fabricante: (OEM, Original Equipment Manufacturer).
    - Partners: (BSP, Board Support Package)
    - Propio: (ODM, Original Design Manufacturers)

Dentro de este ciclo de vida podemos encontrar que el fabricante tiene toda la infraestructura necesaria para implementar IoT como es el caso Amazon AWS[29]. Dentro de los IoT podemos encontrar en su hardware sistema operativos o programación embebida (mircrocontrolador), y dentro estos un stack protocolos de comunicación y mensajería como se observan en Figura 8:

[28] LI DA XU & LI, Securing the Internet of Things, 2017, Aspectos de seguridad IoT.
[29] AMAZON AWS, Internet de las cosas, 2017.

Figura 8 Stack Messaging & Communication



VAN DUREN & RUSSELL, Practical Internet of Things Security, 2016.

La figura anterior proporciona una vista de los protocolos conocidos que pueden implementar con dispositivos IoT[30]. En cuanto términos de seguridad podemos encontrar unas categorías en las cuales los ataques o riesgos de seguridad se agrupan:

- Reconocimiento y mapeo inalámbrico
- Seguridad en protocolos
- Seguridad física
- Seguridad en las aplicaciones

En términos de seguridad cada capa puede estar protegida de acuerdo con sus necesidades, en las capas superiores a la uno (1), la característica de los equipos cambia y estos pueden albergar sistemas de seguridad estándares sin las restricciones que ofrece un “objeto inteligente” de la capa uno. Uno de los objetivos específicos de este trabajo es proponer un diseño basado en los análisis de las diferentes modelos de arquitectura para IoT.

[30] VAN DUREN & RUSSELL, Practical Internet of Things Security, 2016, Figura 8, stack de comunicación y mensajería.

1. DISPOSITIVOS

1.1. Hardware

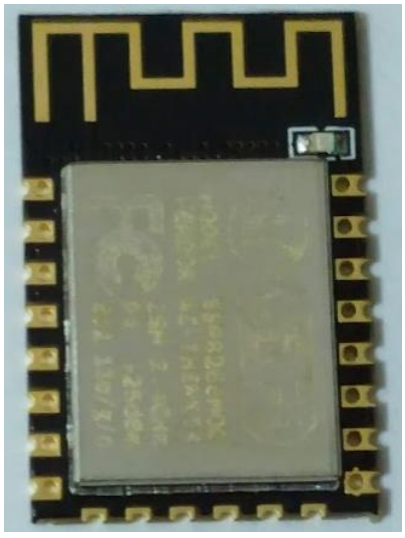
El hardware en el internet de los objetos varía dependiendo del ambiente en el cual se va a desarrollar la solución, en el cual encontramos propuestas profesionales y trabajos personales o comunidad “maker” (hazlo tú mismo), en la cual hardware puede estar clasificado por el tipo de controlador que se esté usando[31]. Algunos dispositivos IoT son usados como asistentes virtuales (véase el Anexo A).

1.2. System On Chip (SOC)

Son microcontroladores integrada (MCU – Microcontroller Unit) los cuales tiene entradas y salidas de propósito general.

Existen plataformas como Arduino, Atmel y sistemas basados en ARM, y otras plataformas como ESP8266 y Node-MCU

Figura 9 ESP8266



Fotografía tomada por el autor.

[31] BARRANCO, Benoit 2018.

Figura 10 Node MCU - Como un ESP8266 Integrado

Fotografía tomada por el autor.

Listado:

- Texas Instruments - CC3220SF-LAUNCHXL.
- STMicroelectronics - STM32L4 Discovery kit IoT node.
- NXP - LPC54018 IoT Module.
- Microchip - Curiosity PIC32MZEF.
- Espressif - ESP32-DevKitC, ESP-WROVER-KIT.

1.3. Industrial Microcontroller (PLC and RTU)

En la parte industrial podemos encontrar dos clasificaciones:

- RTU - Remote Microcontroller Unit
- PLC – Programmable logic controller

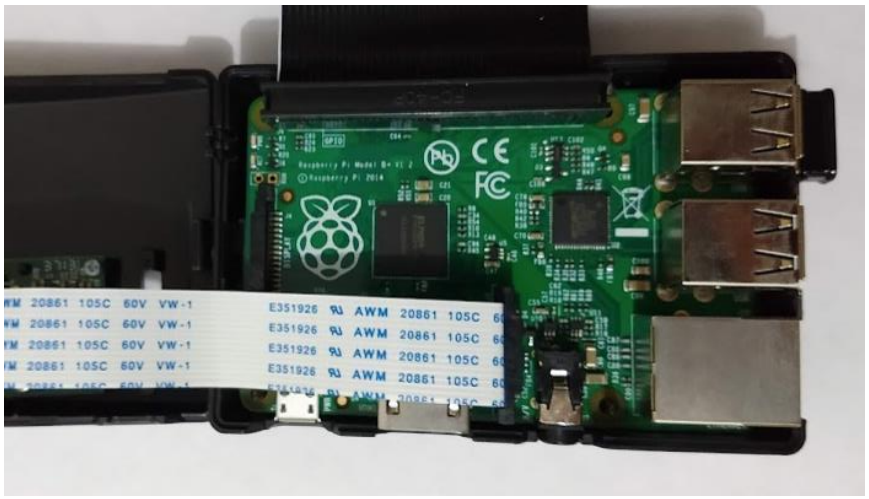
Estos controlan procesos de manufacturación, como líneas de ensamblaje dispositivos robóticos y otras actividades.

1.4. Single Board Computer (SBC)

Es un board de circuito con microprocesador, memoria, entra y salidas y características adicionales, en si son computadores de múltiples usos. Existe una gran cantidad de SBC pero los más destacados son:

- Raspberry Pi
- BeagleBoard
- BananaPi
- Odroid

Figura 11 Raspberry PI



Fotografía tomada por el autor.

Figura 12 Raspberry Pi Zero W

Fotografía tomada por el autor.

1.5. Sensores

Existe una gran cantidad de sensores y de diferentes calidades, los cuales se conectan por diferentes protocolos al hardware que se esté usando en el momento, en el listado a continuación encontramos una gran variedad de ellos:

- Sensores de proximidad
- Acelerómetro y giroscopio
- Sensores de temperatura
- Sensor de humedad
- Sensor de presión
- Sensor de nivel

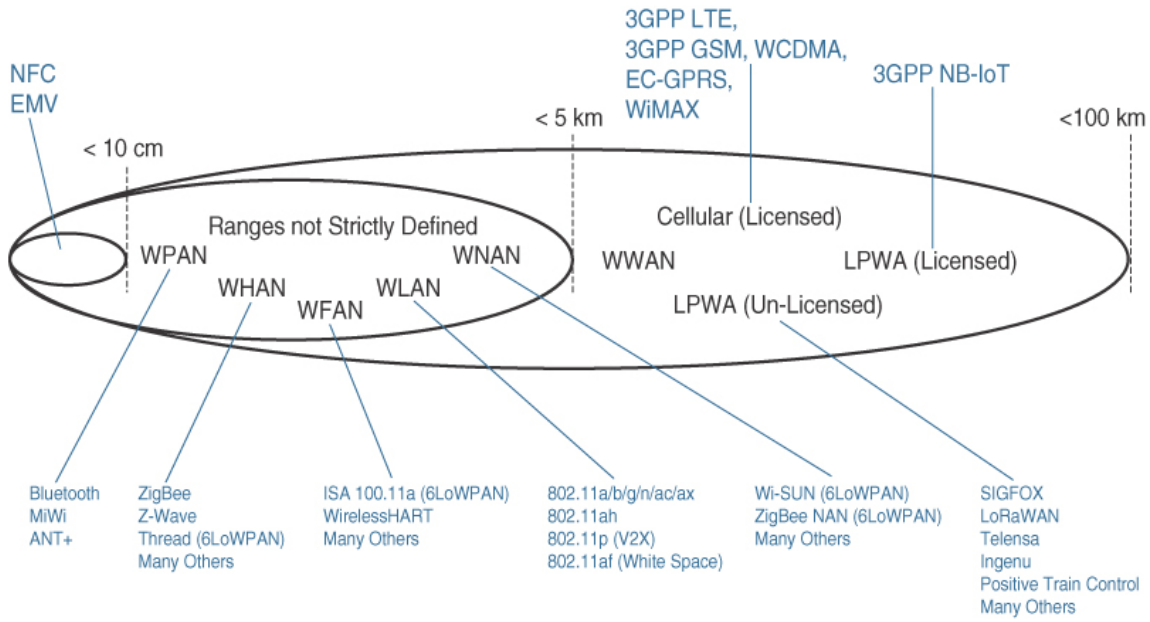
No olvidar que existen los llamados sensores inteligentes los cuales viene integrados con al tipo de hardware antes mencionado.

2. PROTOCOLOS DE COMUNICACIÓN

2.1. Definiciones

Dentro de los dispositivos IoT se encuentran una gran variedad de protocolos de comunicación que se muestran en la siguiente imagen de acuerdo con su alcance[32]:

Figura 13 Rango de protocolos de comunicación



Barton, Salgueiro, & Hanes, IoT Fundamentals.

Estos protocolos se clasifican según su rango:

- Wireless Personal Area Network (WPAN)
- Wireless Home Area Network (WHAN)
- Wireless Field (or Factory) Area Network (WFAN)
- Wireless Local Area Network (WLAN)
- Wireless Neighborhood Area Network (WNAN)
- Wireless Wide Area Network (WWAN)
- Low Power Wide Area (LPWA)

[32] Figura 2-9 Acess Tecnologies and Distances, de Barton, Salgueiro, & Hanes, 2017

2.2. Inalámbrico

Protocolos inalámbricos usados en el IoT, de acuerdo con su alcance y necesidades en trasmisión de datos:

- WirelessHART - IEC 62591, IEEE 802.15.4
- Bluetooth/LE
- 802.15.4 - low-rate wireless personal area network (LR-WPAN).
- 802.11 WiFi
- Zigbee – Basado en IEEE 802.15.4.
- 6LoWPAN - IPv6 over Low power Wireless Personal Area Networks
- IEEE 1609 WAVE
- 802.15.6 WBAN - Wireless Body Area Network.
- Z-Wave – Comunicación inalámbrica, 800 -900 MHz.
- Thread – Es una red tipo mesh basada en IPv6. De bajo poder. Usando 6LoWPAN.
- LTE - Long Term Evolution
- GPRS - General Packet Radio Service
- CDMA - Code Division Multiple Access
- LoRaWAN - Low Power Wide Area Network, 915MHz América, 868 MHz Europa, 433MHz Asia.
- Sigfox - Industrial, Scientific and Medical ISM radio band 868MHz in Europe and 902MHz in the US.
- NFC - Near Field Communication, ISO 14443 a 13.56 MHz.
- DASH7 – ISO/IEC 18000-7 protocolo a 433 MHz.

2.3. Alámbricos

Protocolos alámbricos conexiones entre sensores y el microcontrolador:

- RS-232 - EIA/TIA RS-232C
- RS-422 - ANSI/TIA/EIA-422-B
- RS-485 - TIA-485-A.222
- I2C - Inter-Integrated Circuit
- UART - Universal Asynchronous Receiver-Transmitter, Transmisor-Receptor Asíncrono Universal.
- SPI - Serial Peripheral Interface,

2.4. Mensajería

Los dispositivos IoT tiene que comunicar sus datos a algún servidor actuando como clientes, estos mensajes son enviados de forma directa usando protocolos estándar o usando algún intermediario como bróker de mensajería[33], existen diferentes tipos de bróker de acuerdo con el fabricante o a la especificación implementada, pero la mayoría son enfocados a ser usado como un sistema de colas tipos publicador/suscritor.

2.4.1. Message Queue Telemetry Transport (MQTT)[34]

Es uno de los más usados protocolos de mensajes en IoT, es soportado por la mayoría proveedores, el cual funciona como una aplicación en la capa del modelo IP. Su principal funcionamiento es el concepto de mensaje donde este es entregado en el servidor, los dispositivos son "Publisher" publicadores y quien consume el mensaje "subscriber" subcriptor.", las conexiones son intermitentes donde los mensajes se manejan topicos "Topics" y no como un bróker tradicional que se manaje en colas. Un tópico es como una ruta del sistema los cuales los publicadores y suscritores acceden a estas.

Ventajas:

- Los paquetes pueden ser texto o binario.
- Confiable
- Escalable
- Diseño desacoplado
- Seguridad, aunque se debe usar con TLS/SSL ya que por defecto no trae seguridad.
- Bidireccional.
- Creado por IBM y dado como proyecto OpenSource.

Desventajas:

- Opera sobre TCP
- Centralizado.
- Único punto de falla.
- Inseguro, los datos no están encriptados por defecto.

[33] Del inglés Message Broker
[34] MINTEER, 2017.

2.4.2. Hypert-Text Transport Protocol (HTTP)[35]

Se usa el protocolo HTTP para transferencia de datos usando los servicios RESTful (Representational State Transfer), usando los métodos del protocolo HTTP como interface para la transferencia de datos POST, GET, PUT, PATCH, DELETE.

Ventajas:

- Confiable
- Fácil implementación.
- Compatible.

Desventajas:

- Alto consumo de energía.
- Se requiere recursos de CPU por la complejidad del protocolo.

2.4.3. Extensible Messaging and Presence Protocol (XMPP)[36]

Es una tecnología abierta para la comunicación en tiempo real, usando Extensible Markup Language (XML), este es usado en una gran variedad de aplicaciones. Usado principalmente en aplicaciones de mensajería, pero lo han estado usando en el intercambio de información de los dispositivos IoT.

Ventajas:

- Seguro
- Descentralizado
- Estandarizado
- Escalable

Desventajas

- Mensajes grandes por el uso de XML.

[35] MINTERR, 2017
[36] PETER SAINT-ANDRE, 2009

2.4.4. Constrained Application Protocol (CoAP)[37]

CoAp[38] es ligero protocolo alternativo a HTTP, el cual puede ser usado en sistemas de poco ancho de banda. Puede usar las operaciones GET, PUT, POST, DELETE, las cabeceras soportan binary a diferencia de HTPP que usa ASCII, maneja los errores 2xx (success, exitoso), 4xx (client error, error en el cliente), 5xx (server error, error en el servidor), y la seguridad basada en DTLS, actualmente soporta UDP y TCP.

Ventajas:

- Protocolo ligero.

Desventajas:

- Es una propuesta y aun no tiene se ha extendido.

2.4.5. Advanced Message Queuing Protcol (AMQP)

Es una especificación abierta para envíos de mensajes asíncronos. Donde cada se envía datos binarios. Se puede usar en múltiples plataformas, y es interoperable entre estas. Y está definido como estándar internacional ISO/IEC 19464[39]. Sigue le modelo publicador/suscritor usando tópicos y colas para el manejo de los mensajes.

Ventajas:

- Garantía de entrega
- Alta disponibilidad
- Tolerancia a fallos
- Asíncronas

Desventajas:

- Algunas implementaciones no tienen el estándar completo.

[37] ZURAWSKI, 2017
[38] RFC 8323 https://tools.ietf.org/html/rfc8323
[39] ISO/IEC, 2014

3. PROCESAMIENTO DE DATOS

3.1. Administración de datos

En la administración de los datos se encuentran sistemas como SCADA que son antecesoras a IoT y que manejen el proceso industrial de muchas empresas, que realizan el mismo proceso de IoT, interactuar con el mundo físico recolectando datos e interactuando con sensores que pueden ejecutar acciones, el mundo conectado de hoy y el abaratamiento tecnológico a llevado a que muchas empresa no industriales comienzan a usar este tipo de tecnología para optimizar sus procesos y mejoramiento de los existentes. La administración de los datos se vuelve vital y el uso de diferentes tecnologías dan que surjan diferentes conceptos en la administración de los datos.

3.1.1. SCADA

Previo al inicio del llamado IoT, los procesos industriales usan un sistema denominado SCADA[40] (Supervisory Control And Data Acquisition o Control con Supervisión y Adquisición de Datos), el nombre es dado a cualquier software que permita el acceso a datos remotos de un proceso y permitan de alguna forma el control de este.

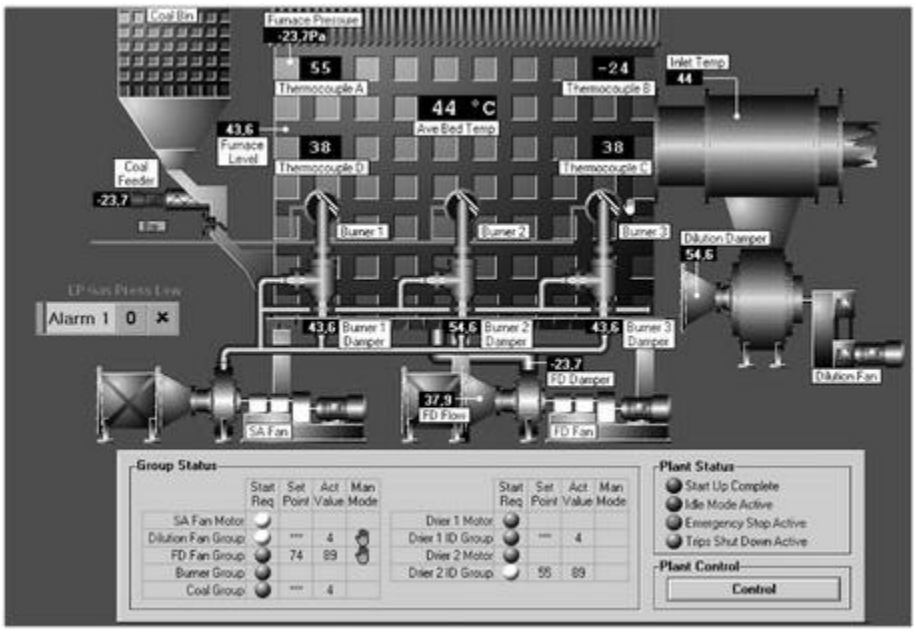
Prestaciones:

- Monitorización
- Supervisión
- Adquisición de datos de los procesos de observación
- Visualización de los estados de las señale del sistema. (eventos y alarmas).
- Tener Mando
- Seguimiento de instrucciones programadas
- Seguridad en los datos
- Seguridad de ingresos

[40] RODRÍGUEZ PENIN, 2012

En l siguiente figura se encuentra una pantalla de ejemplo de un panel Sinóptico de un horno[41]:

Figura 14 Pantalla de Monitorio SCADA



Rodríguez Penin, 2012.

3.2. Cloud Computing

Según la NIST[42], la computación en la nube es un modelo que permite acceso ubicuo, conveniente y bajo de manda a conjunto compartido de recursos (almacenamiento, redes, servidores, servicios y aplicaciones) que se puedan aprovisionar y lanzar de forma rápida con un mínimo esfuerzo del proveedor. El cual está compuesto de:

Características esenciales:

- On-demand sel-service.
- Acceso a red de banda ancha.
- Agrupación de recursos.
- Rápida flexibilidad[43]
- Medidor del servicio

[41] Figura 38 – Panel Sinóptico de un horno (realizado con WinCC, Siemens), de Rodríguez Penin, 2012.
[42] National Institute of Standards and Technology U.S Department of Commerce, Instituto Nacional de Estándares y Tecnología, departamento de comercio de los Estados unidos; MELL & GRANCE 2011.
[43] Se refiere a elasticidad de la demanda – Rapid elasticity.

Modelo del Servicio:

- Software como un servicio[44].
- Plataforma como un servicio[45]
- Infraestructura como un servicio[46]

Modelo de despliegue:

- Nube privada
- Nube en comunidad
- Nube publica
- Nube hibrida

Se puede resumir que la computación en nube (Cloud Computing), está diseñada para ser ofrecida como un servicio en la cual su cobro esta por el uso de recursos y que debe garantizar una cuantificación de estos para garantizar un uso efectivo de los recursos que se requieren, adicionalmente un proveedor de estos servicios puede tener:

- Disponibilidad de recursos.
- Capacidad de clientes diversos y heterogéneos.
- Agrupación de recursos.
- Elasticidad y dinamismo.
- Suministros proporcionados como servicios.

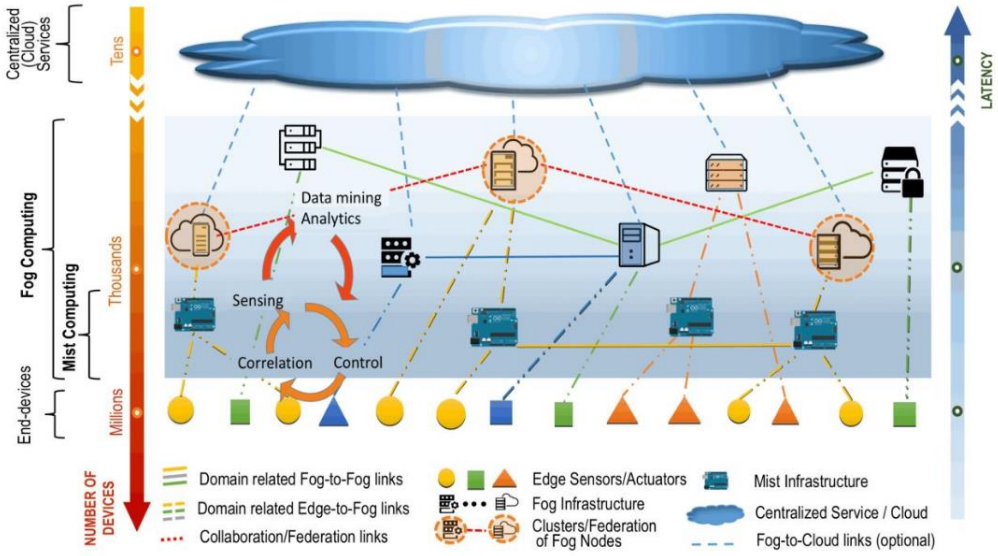
Dentro diferentes proveedores se pueden encontrar servicios orientados al internet de las cosas, los cuales ofrecen diferentes soluciones de acuerdo con sus necesidades.

3.3. Fog Computing

Según la NIST[47], es un multi-capa que tiene acceso ubicuo a un conjunto de escalables recursos de computación. Este modelo facilita el despliegue distribuido, baja latencia y aplicaciones y servicios que consisten en “fog nodes”, tanto fisicos como virtuales entre dispositivos[48] y servicios en la nube centralizados.

[44] SaaS - Software as a Service
[45] PaaS - Platform as a Service
[46] IaaS – Infrasreucture as a Service
[47] National Institute of Standards and Technology U.S Department of Commerce, Instituto Nacional de Estándares y Tecnología, departamento de comercio de los Estados unidos, LORGA 2018.
[48] Smart end-devices, en referencia a dispositivos de internet de las cosas.

Figura 15 Fod Computing



LORGA 2018.

Los “fod node” son componentes que se unen de forma estrecha a los dispositivos y los servicios de computo (gateways, switches, routers, servers, etc.), Cada nodo puede estar geográficamente distribuida y con capacidades diferentes.

Características esenciales:

- Ubicación local y baja latencia.
- Distribución geográfica diversa.
- Heterogenia.
- Interoperabilidad y federación.
- Interacciones en tiempo real.
- Escalabilidad, federación ágil y clúster de fod-node.

Características asociadas:

- Acceso predominante inalámbrico.
- Soporte para movilidad.

Atributos:

- Autonomía

- Heterogeneidad
- Estructura en clúster
- Manejabilidad
- Programación

Modelo de servicios:

- Software como servicio[49]
- Plataforma como servicio[50]
- Infraestructura como servicio[51]

3.4. Edge Computing

Es el procesamiento de los datos cerca a la fuente de generación, en lugar de enviarlos a otro lado a procesar. Edge Computing es una arquitectura abierta y distribuida que realiza su procesamiento descentralizado permitiendo la computación móvil y el internet de las cosas, los datos pueden ser procesados por el propio dispositivo o por un servidor/computador local[52].

3.5. Grid Computing

Grid Computing, usa una red computadores heterogéneas interconectadas para el procesamiento de datos, estos equipos están separados geográficamente[53].

3.6. Ubiquitous computing

Ubiquitous computing o *ubicomp*, es el termino dado a la era de la computación moderna[54], donde el enfoque a es la gran cantidad de pequeños dispositivos como teléfonos inteligentes, asistentes personales, computadores embebidos y como resultados el uso de muchos computadores[55].

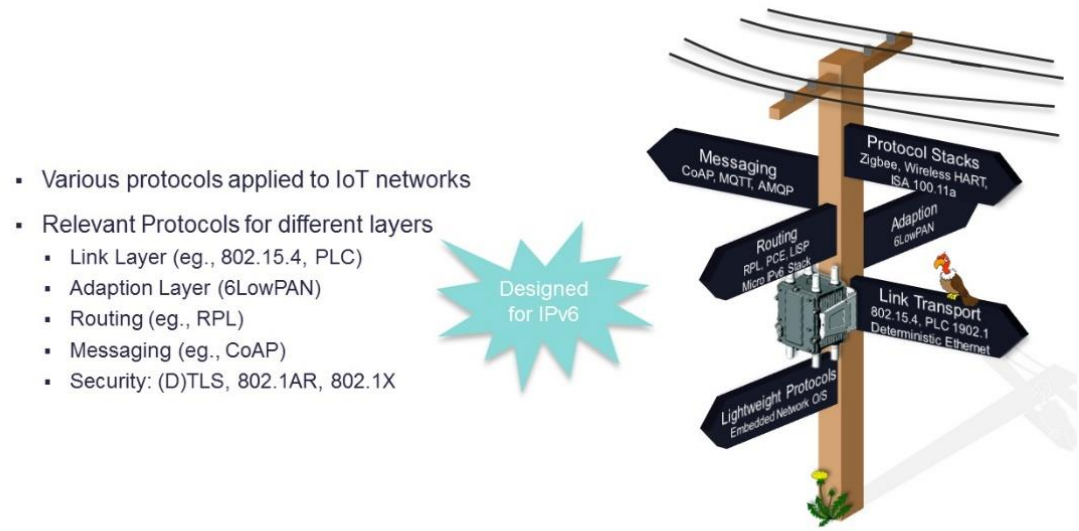
[49] SaaS - Software as a Service
[50] PaaS - Platform as a Service
[51] IaaS – Infrasreucture as a Service
[52] HEWLETT PACKARD ENTERPRISE, 2018
[53] WILKINSON, 2009
[54] La primera de ña computación definidad como "mainframe computer", la se gunda era como el computador personal PC-Personal Computer.
[55] KRUMM, 2016

4. SEGURIDAD

4.1. Definiciones

En las secciones anteriores se ha descrito protocolos, dispositivos y formas de procesamiento de datos, los cuales son muy variados y en algunos casos antiguos con adaptaciones para el mundo moderno basado en IoT, como se observa en la siguiente imagen[56][57][58][59]:

Figura 16 Muestras de Protocolos IoT



Cisco, 2017.

Esta gran diversidad presenta desafíos dentro de los sistemas IoT, los cuales listamos a continuación:

- Dispositivos económicos y pequeños, con o sin seguridad física.
- Dispositivos que no tiene recursos suficientes de computo, no pueden admitir algoritmos de seguridad complejos.

[56] Imagen tomada de Cisco, 2017.
[57] RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, RFC 6550.
[58] A Path Computation Element (PCE)-Based Architecture, RFC 4655
[59] The Locator/ID Separation Protocol (LISP), RFC 6830

- ❖ Administración de múltiples redes
- ❖ Crypto Resiliencia
  - o Algoritmos criptográficos tiene corta duración.
- ❖ Protección Física
  - o Dispositivos móviles pueden ser robados
  - o Dispositivos fijos, los pueden mover.
- ❖ Técnicas de detección de sabotaje.
- ❖ Suministro eléctrico.
- ❖ Conexión y desconexión a la red.

4.2. Amenazas de IoT

Las amenazas actuales como Smurfing, Spoofing, Fragmentation attacks, Hombre en el medio entre otros, y requiere de la misma seguridad de los computadores y dispositivos móviles actuales.

Un virus para computadora se queda en es punto, se puede propagar, pero, aunque haga daños, algunos son reparables, pero se quedan, en ese mundo virtual, a diferencia de IoT que interactúa con el físico y que puede ocasionar daños a las personas, un ejemplo sería el control de tráfico, poner los semáforos en verde en una intersección al mismo tiempo provocaría accidentes. Podemos encontrar algunas categorías:

- Gusanos que salten a IoT
- Ataques a IoT residencial
- Crimen organizado (ej: sabotaje)
- Ciber terrorismo.

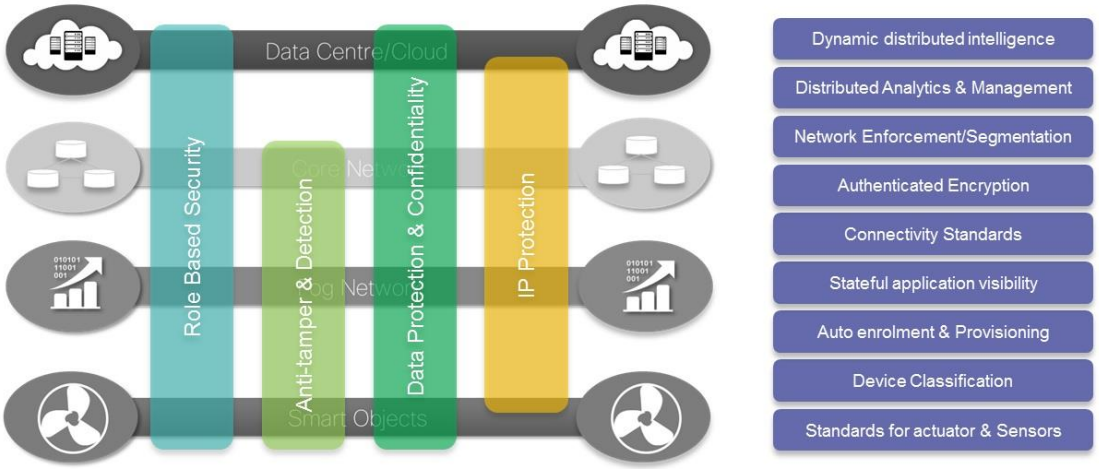
Uno de los elementos fundamentales para la seguridad es la identificación del dispositivo y los mecanismos para autenticarla, pero como se ha mencionado, algunos dispositivos IoT no tiene la potencia de computo necesaria para procesar algoritmos criptográficos, por tal motivo ser requieren de nuevas formas de protección para adaptarse a un nuevo mundo conectado a IoT.

4.3. Framework de seguridad

4.3.1. Framework de Seguridad Cisco

El marco de trabajo[60] requiere una seguridad flexible y se ilustra en la siguiente imagen:

Figura 17 Entorno de Seguridad IoT



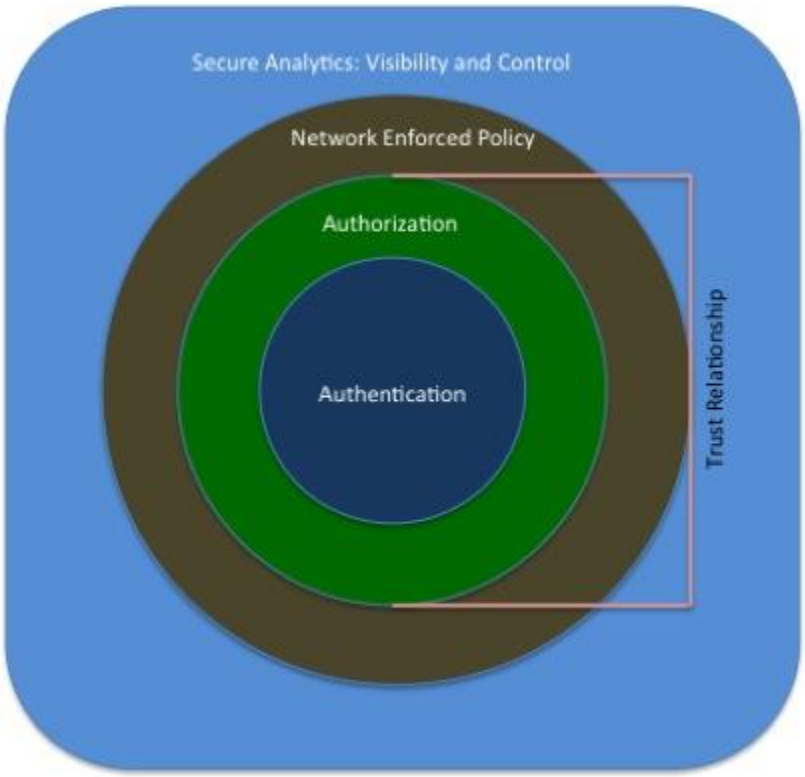
CISCO, 2017.

Este marco de trabajo se compromete en 4 componentes:

1. Autorización
2. Autenticación
3. Análisis seguro: Visibilidad y Control
4. Política aplicada a la red

[60] CISCO, 2017.

Figura 18 Marco Seguro de IoT



Cisco, 2017.

Autenticación

Identificar los dispositivos IoT sin la necesidad de la interacción humana deben de incluir RFID (identificación por radiofrecuencia) , clave compartida, certificados X.509, dirección MAC del dispositivo o algún tipo de certificado de confianza que no se pueda modificar basada en hardware. Para dispositivos que no soportan lo anterior pueden usar el estándar 802.1AR y los protocolos de autenticación definidos por IEEE 802.1X, se puede aprovechar para aquellos dispositivos que pueden administrar tanto la carga de la CPU como de memoria de almacenamiento.

Autorización:

Se establece una relación de confianza con los componentes de autenticación y autorización, entre los dispositivos de IoT para intercambiar información apropiada.

Se aplican políticas y controles apropiados para segmentar la red y establecer comunicación de extremo a extremo de forma segura en toda la red.

Política aplicada a la red

La capa contiene los elementos que pueden enrutar y transportar el tráfico de dispositivos de forma segura a través de la infraestructura, ya sea control, gestión o tráfico de datos real. Aplicando protocolos y mecanismo existentes.

Análisis Seguro: Visibilidad y Control

En la capa se definen los servicios en los cuales pueden participar todos los componentes, la mitigación de amenazas puede variar desde apagar automáticamente al atacante para que no acceda a recursos adicionales a ejecutar scripts especializados para mitigar el impacto.

Este marco de seguridad da la base a partir del cual se puedan seleccionar los servicios de seguridad apropiados. A medida que se consideran contextos y verticales específicas, se pueden identificar y abordar las brechas.

5. ARQUITECTURAS

5.1. Definiciones

En el marco conceptual y teórico se mencionaron algunas arquitecturas, en los siguientes ítems se adicionará información relacionada no presentada.

En los siguientes modelos presentados, el tema de seguridad es capa transversal y que se vuelve omnipresente he inherente a las arquitecturas y tecnologías usadas.

5.2. Arquitecturas con siete capas

5.2.1. Modelo IoTWF

El modelo IoTWF[61] Como se visualiza en la Figura 2 (ver pág. 20), el modelo de siete (7) capas descrito en la tabla Tabla 1 (ver pág. 21) describe una básica premisa:

Los dispositivos envían y reciben datos interactuando con la red donde la data es trasmitida, normalizada y filtrada usando Edge Computing antes de ser almacenada (Base de Datos) que es accesible por aplicaciones la cual procesa y provee a las personas para que pueda actuar y colaborar.

Como se observa en la premisa, está basada en un flujo de información, donde su punto central está en la tecnología y los dispositivos, desacoplamiento, interoperabilidad, análisis e integración con la empresa.

Usando un término de Edgeware[62], para Edge Computing, donde este puede estar separado de la capa de aplicación, ya que es un software (conjunto de programas) para la interacción con los dispositivos. Podemos encontrar:

- Control de dispositivos: Configuración y estatus.
- Interacción de dispositivos: Descubrimiento y direccionamiento.
- Middleware: Listeners (Zigbee), bróker (MQTT).
- Datos: Normalización decodificación, agregación, notificación y alertas.
- Combinación de funciones: Como tareas programadas y BPM.
- Seguridad: Roles y Privilegios.

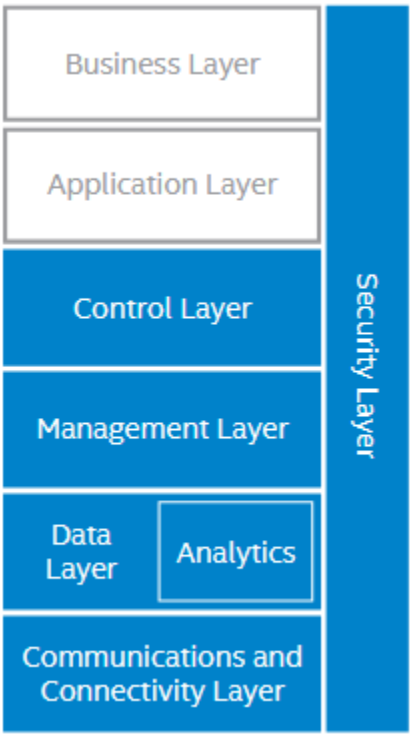
[61] CISCO, 2014. IoT World Forum Reference Model.
[62] Edgeware = Edge Software

5.3. Arquitecturas de seis capas

5.3.1. Intel IoT Platform Refrence Arquitecture

La arquitectura de IoT de Intel[63] es por capas en las cuales tiene una componente transversal de seguridad ligado a cada capa. Como se visualiza en la siguiente figura:

Figura 19 Arquitectura IoT Intel



INTEL, 2015.

Descripción de las capas más importantes:

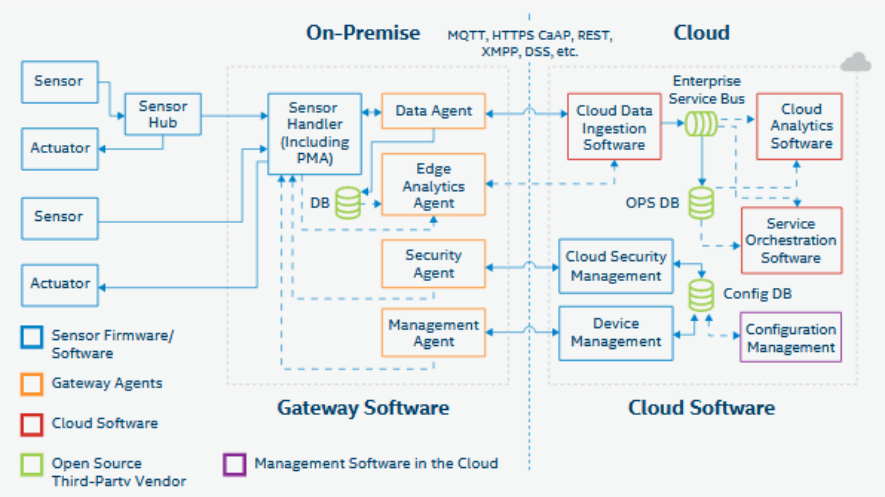
- Commnunications and Connectivity Layer – Capa de comunicaciones: usar múltiples protocolos entre diferentes tipos de dispositivos, conectados mediante una red PAN/LAN o WAN.

[63] INTEL, 2015. Intel® IoT Platform Reference Architecture.

- Data Layer with Analytics – Capa de datos con análisis: Esta capa se enfoca a usar Egde Computing para el control de los datos.
- Management Layer – Capa de gestión: Gestión sobre los dispositivos, supervisando las operaciones.
- Control Layer – capa de control: Separado de la gestión se tiene el control del acceso a los dispositivos y políticas de seguridad.
- Security Layer – Capa de seguridad: protección robusta de principio a fin en cada capa, usando diferentes formas de seguridad dependiendo de la capa que se esté protegiendo.

En la siguiente figura se muestran dos grandes grupos, el primer grupo corresponde a los sensores (dispositivos IoT) y a los Gateway, el segundo grupo corresponde a la computación en la nube. Los componentes en la nube son responsables de la gestión de datos desde el dispositivo, almacenamiento de datos análisis de datos, gestión del servicio y seguridad.

Figura 20 Componentes de software e interfaces referencia IoT



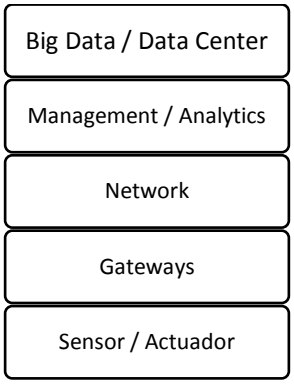
INTEL, 2015.

5.4. Arquitectura de cinco capas

5.4.1. IoT Simple

Esta es una empresa[64] que presenta un modelo de cinco capas interrelacionadas:

Figura 21 Modelo IoT Simple



IOT SIMPLE, 2018.

- Capa 1 – Sensor/Actuador: Dispositivos tipo sensor o actuadores.
- Capa 2 – Gateways: Soporte a los dispositivos que no cuenten con conexiones TCP IP.
- Capa 3 – Network: Manejo de la red empresarial.
- Capa 4 - Management / Analytics: Administración de los datos recolectados.
- Capa 5 – Big Data / Data Center: Capacidad de almacenamiento y procesamiento de información.

La seguridad es transversal a las cinco capas, donde tiene un enfoque físico y lógico. Donde integran:

- Autenticación.
- Filtrado.
- Encriptación.
- Protección.

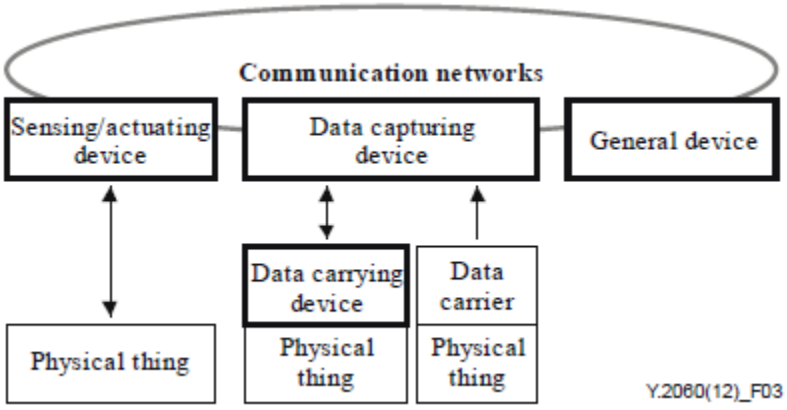
[64] IOT SIMPLE, 2018.

5.5. Arquitecturas de cuatro capas

5.5.1. Modelo ITU

Como se mostró en la figura del modelo de ITU[65] (ver Figura 3, pág. 22) es un modelo de cuatro (4) capas donde tiene dos capacidades transversales para la gestión y seguridad. En la figura siguiente se muestra la relación entre los dispositivos y los objetos(cosas) físicos.

Figura 22 Relación de dispositivos objetos físicos.



ITU-T Y.2060

Profundizando en estas capas transversales encontramos:

Capacidad de Gestión:

- Gestión de dispositivos, desactivación y activación de forma remota, diagnóstico y actualización de software.
- Gestión de topología de la red.
- Gestión de tráfico de la red.

Capacidad de Seguridad:

[65] ITU-T Y.2060, IoT Reference Model.

- Capa de aplicación: autenticación, autorización, integridad, privacidad, auditorias, antivirus.
- Capa de red: confidencialidad, autenticación, autorización.
- Capa de dispositivo: autorización, control de acceso, autenticación, confidencialidad y protección de datos.

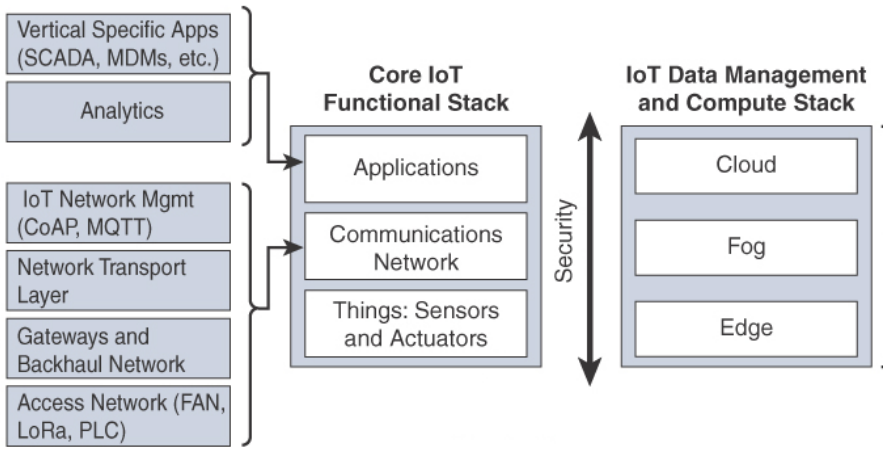
Las capacidades de seguridad y de gestión pueden estar específicamente relacionas con los requisitos de la aplicación, es decir, con la data que se puede manipular, en otras palabras, que tan sensible son los datos que se van transportar.

5.6. Arquitecturas de tres capas

5.6.1. Modelo de Barton, Salgueiro, & Hanes.

Este modelo no intenta ser un marco de trabajo para una arquitectura de IoT como lo indica en el libro, sino que presenta los bloques principales en los cuales se fundamenta la mayoría de los ecosistemas IoT. En la siguiente figura se expande este modelo de tres capas en varias subcapas[66]:

Figura 23 Arquitectura expandida



Barton, Salgueiro, & Hanes, 2017.

[66] Basada en la figura 2-7 Expanded View of the Simplified IoT Architecture, Barton, Salgueiro, & Hanes, 2017.

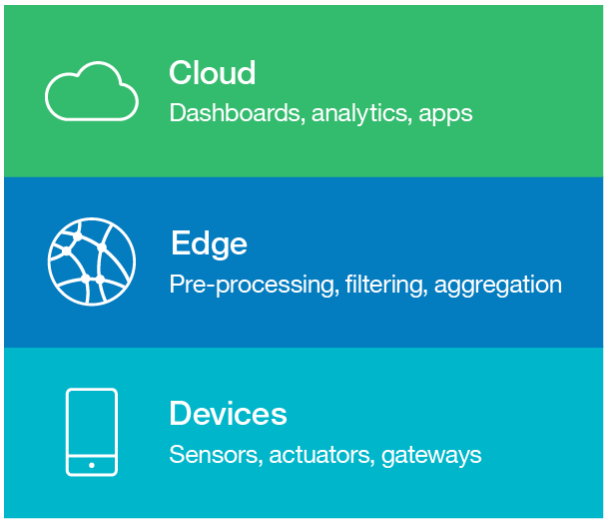
En las sub-capas encontramos:

- Access Network: Denominado como “Last mile” encontramos las conexiones a los sensores.
- Gateway and Backhaul Network: Este actúa como una aplicación que recolecta los datos de la capa inferior.
- Network transport: Esta es la capa esta dar de protocolos TCP/UDP IP.
- IoT network management: Intercambio de datos con los sensores usando algún tipo de mensanjeria CoAP y/o Broker.
- Aplicaction and analytics: Corresponde a la capa de negocio donde se procesan y se usan aplicaciones para la toma de decisiones.

5.6.2. Arquitectura de Referencia de IoT de IBM

La arquitectura de IBM es un modelo base de tres (3) niveles donde se integran otras capas transversales como la gestión de identidades o seguridad de los datos. En la figura siguiente se visualizan estas capas base[67]:

Figura 24 Capas de Arquitectura IoT IBM



GERBER, 2017.

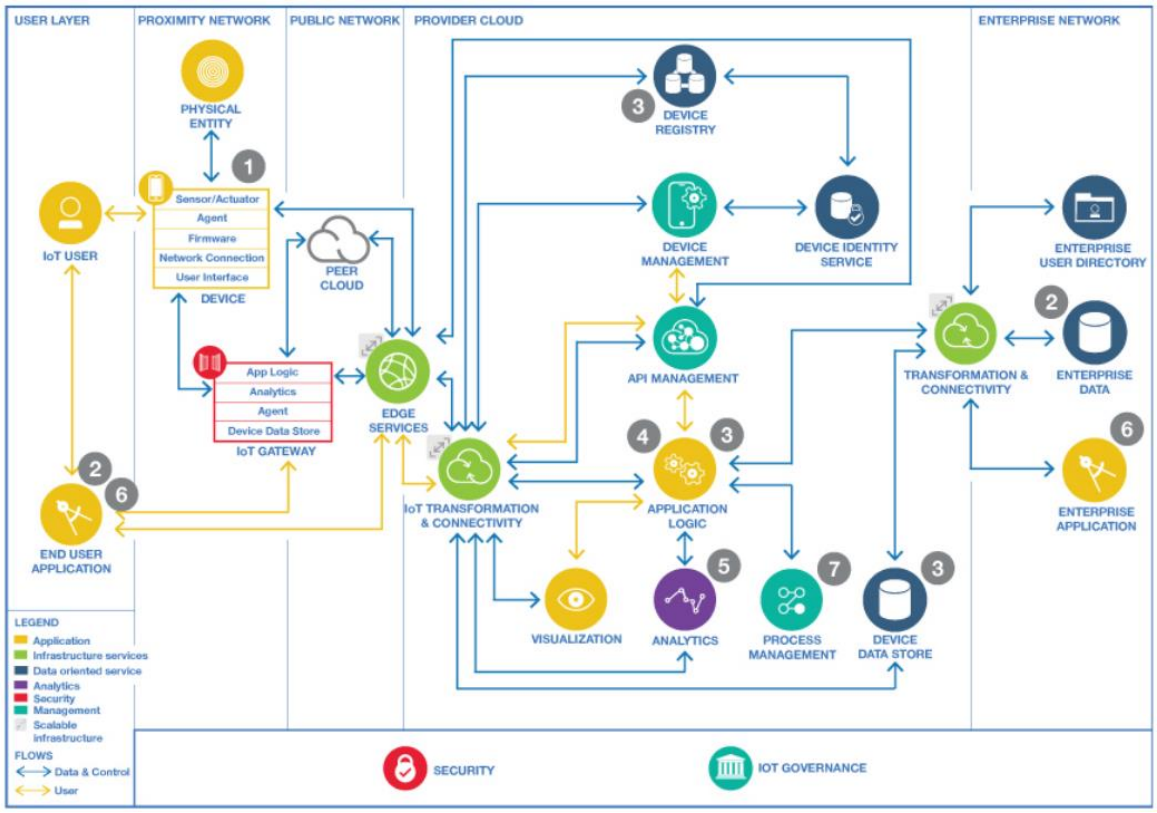
[67] GERBER, 2017.

Estas capas en la arquitectura agrupan más subcapas que otras arquitecturas en etas se encuentran las siguientes descripciones:

- Capa de Dispositivos (Devices)
- Capa Edge
- Capa de nube (Cloud)

Esta arquitectura tiene un foque de Edge Computing para disminuir la latencia y filtrado de datos que se dirigen en la nube, ampliando la arquitectura podemos observar la siguiente imagen[68]:

Figura 25 Arquitectura de Referencia IBM.



IBM, 2018.

[68] IBM, 2018. IoT reference architecture.

Donde se detalla los siguientes Ítems:

1. Sensores y actuadores.
2. Autorizaciones y logs.
3. Servicios en la nube para la data.
4. Registros de dispositivos.
5. Análisis de datos.
6. Aplicaciones para la toma de decisiones.
7. Respuesta a la toma de decisiones.

Este modelo incluye la interacción con el usuario por medio de dispositivos móviles, controlando y analizando los datos generados por las aplicaciones que recolectaron la información de los diferentes dispositivos/sensores, donde la información que se integra en la nube ha sido filtrada por una capa de pre-procesamiento (Edge Computing) antes de almacenarse y un procesamiento por los diferentes herramientas que puedan dar la gestión y responder a los eventos generados por los diferentes dispositivos informando de forma temprana a los usuarios finales.

El modelo de referencia de arquitectura de IBM para IoT es un enfoque comercial para el uso de sus propios productos como IBM BPM[69], IBM Cloud, IBM Broker, IBM Monitor entre otros.

5.6.3. Azure IoT Reference Architecture

La arquitectura de referencia Microsoft Azure IoT[70], esta bsad como una solución para ser usado con Microft Azure, el cual se ve como un flujo de datos, donde la meta de la arquitectura es tomar acciones de acuerdo con los datos que se han recopilado.

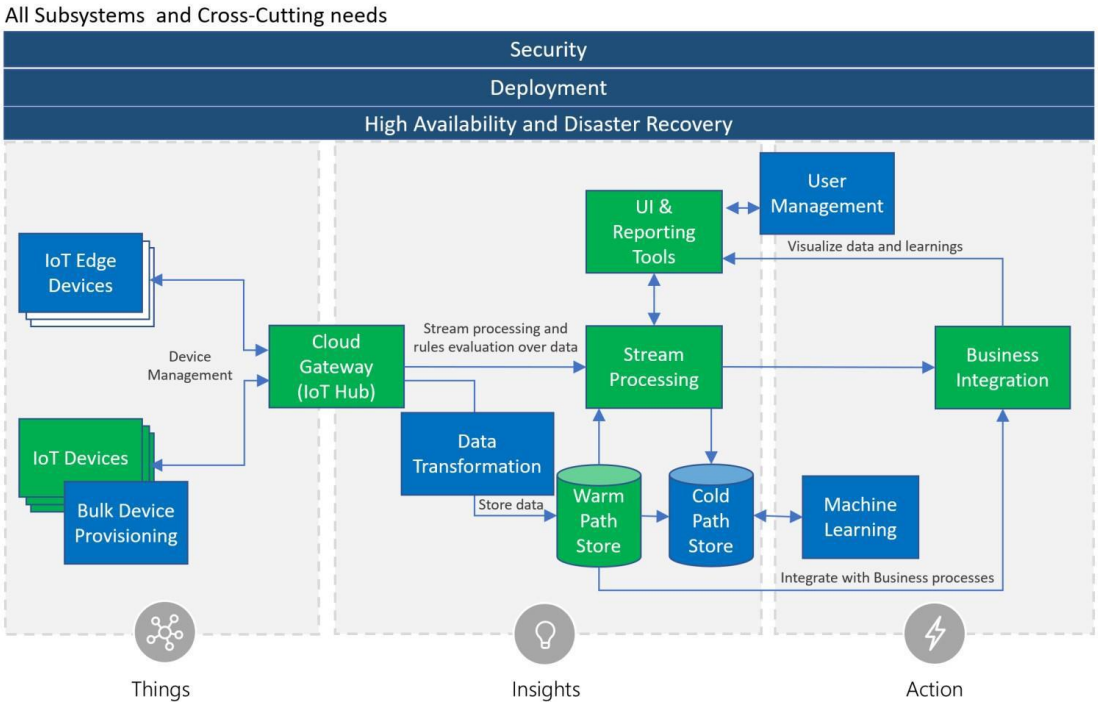
Figura 26 Flujo de Datos - Azure IoT

MICROSOFT, 2018.

[69] BPM – Business Process Management, Gestión de Procesos de Negocio.
[70] MICROSOFT, 2018

Donde su modelo completo se representa de la siguiente forma:

Figura 27 Arquitectura Azure



MICROSOFT, 2018.

La arquitectura manejo los siguientes principios:

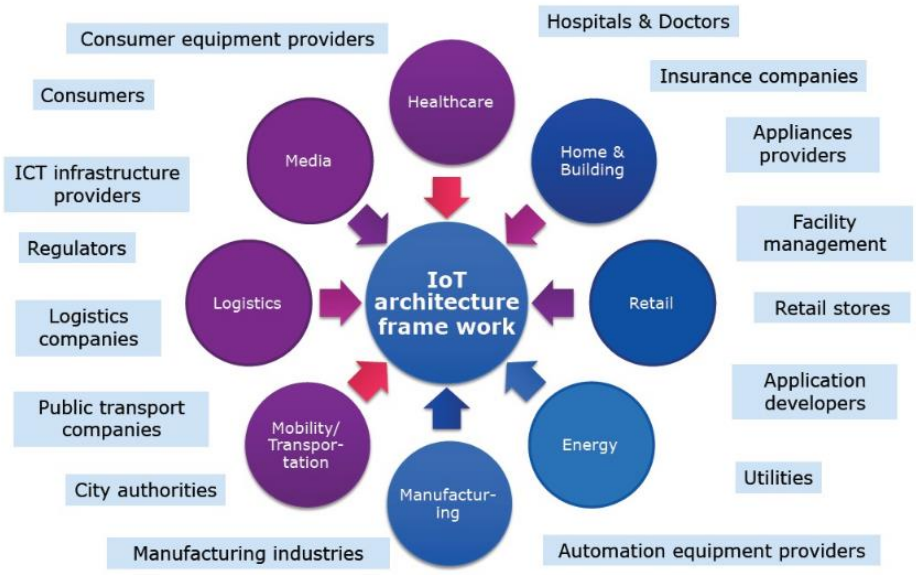
- Heterogeneidad
- Seguridad
- Gran escala
- Flexibilidad

Esta arquitectura también ofrece Egde Computing, el cual se denomina “intelligen Edge devices” el cual hace un preprocesamiento de información mejorando las funcionalidades encontradas. La conexión entre los dispositivos se realiza por medio algún “Gateway” con el fin de realizar conexión es seguras donde las conexiones se realizan en diferentes fuentes. Y como en el modelo de IBM, se basan en una solución basada en sus productos.

5.6.4. Modelo IEEE

El modelo IEEE P2413[71] está considerando un modelo de tres de capas (ver Figura 5, pág. 23) con la idea de que este framework[72] se usado por stakeholders[73] y el mercado actual como se muestra en la siguiente figura:

Figura 28 IoT mercado y stakeholders.



IEEE, 2015.

El interés es que pueda tener: protección, seguridad, privacidad y que sea seguro, a su vez que sea posea Interoperatividad y compatible con otros sistemas a la fecha[74] solo sigue siendo un borrador.

[71] IEEE, 2015. Towards a Definition of the Internet of Things (IoT).
[72] Framework: Marco de Trabajo
[73] Personas involucradas e interasadas
[74] 2018-Octubre-17

6. DISEÑOS RECOMENDADOS

6.1. Definiciones

Se han expuesto ocho (8) modelos de arquitecturas de IoT, en que tres modelos son genéricos y los otros corresponden a la oferta de IoT como un servicio, donde especifican que algunos componentes pueden ser genéricos y otros de su propia marca. Todos ofrecen una seguridad inherente a la tecnología usada.

Hay un punto en común en la mayoría de los modelos, es que no exponen de forma directa los dispositivos IoT (al menos que no sea móvil), y que exista un previo procesamiento antes de que la data se almacene (en la nube).

Modelos Genéricos:

- Modelo ITU
- Modelo IEEE
- Modelo de Barton, Salgueiro, & Hanes

Modelos Comerciales:

- Modelo IoTWF
- Intel IoT Platform Refrence Arquitecture
- IoT Simple
- Arquitectura de Referencia de IoT de IBM
- Azure IoT Reference Architecture

El modelo IoTWF actúa como un modelo genérico su enfoque es comercial, ya que toma de la industria su modelo con el fin de mostrar el estado actual de la industria y no un modelo general para su adopción.

El Modelo IEEE es un borrador que no ha sido publicado como un estándar y sigue en proceso de refinamiento.

En la siguiente tabla se describen algunas características de los modelos y/o arquitectura:

Tabla 2 Tabla de comparación entre modelos de IoT

Modelo	Numero de Capas	Capa de Seguridad Transversal	Cloud Propia	Usa productos propios.	Edge
ITU	4	SI	NO	NO	NO ESPECIFICA
IEEE	3	SI	NO	NO	NO ESPECIFICA
Barton, Salgueiro, & Hanes	3	SI	NO	NO	SI
IoTWF	7	SI	NO	PARTNER	SI
Intel	6	SI	SI	SI	SI
IoT Simple	5	SI	SI	SI	PARCIAL
IBM	3	SI	SI	SI	SI
Azure	3	SI	SI	SI	SI

Autor, diferencia en características.

Todos los modelos y/o arquitecturas garantizan las siguientes características:

- Seguridad.
- Interoperatividad:
  - Entre Dispositivos.
  - Entre Componentes de Software
- Análisis de datos.
- Almacenamiento de información.
- Flexibilidad
- Escalabilidad
- Control de dispositivos.

6.2. Arquitecturas recomendadas

Para determinar las arquitecturas recomendadas validaremos los siguientes puntos:

- [1] Capa transversal de seguridad.
- [2]Administrable.
- [3]Interoperable
- [4]Heterogéneo.
- [5]Independiente de un fabricante.
- [6]Compatible con proveedores de plataforma.

Tabla 3 Selección del Modelo de Referencia

Modelo	1	2	3	4	5	6
ITU	SI	SI	SI	SI	SI	SI
IEEE	SI	SI	SI	SI	SI	SI
Barton, Salgueiro, & Hanes	SI	SI	SI	SI	SI	SI
IoTWF	SI	SI	SI	PARCIAL	PARCIAL	PARCIAL
Intel	SI	SI	PARCIAL	PARCIAL	NO	PARCIAL
IoT Simple	SI	SI	PARCIAL	PARCIAL	PARCIAL	PARCIAL
IBM	SI	SI	PARCIAL	PARCIAL	NO	PARCIAL
Azure	SI	SI	PARCIAL	PARCIAL	NO	PARCIAL

Autor, selección del modelo de referencia.

Analizando los anteriores parámetros podemos inferir de la Tabla 3, que la condición «Independiente de plataforma» deja por fuera a los modelos comerciales, es decir, no implementar una suite completa de algún fabricante ya que puede que las necesidades no sean la esperadas, otro punto negativo son los esfuerzos en crear integraciones para hacer que otros sistemas funcionen con un modelo propietario.

EL modelo de la IEEE sigue siendo un borrador y no un estándar aprobado, así que puede tener variaciones y definiciones sobre sus capas, aunque podemos tomar características para mejorar nuestra implementación de una arquitectura IoT.

El modelo explicado en el libro Barton, Salgueiro, & Hanes, no intenta ser una arquitectura de referencia, pero explica capa por capa que es lo que debería de tener, aunque su modelo de tres (3) capas explica es similar a otros da una visión entera de este tipo de arquitecturas.

De las arquitecturas se pueden recomendar dos modelos:

1.- Modelo ITU

2.- Modelo de Barton, Salgueiro, & Hanes

Aunque estos modelos se ven a simple vista simplificados, la estructura de las subcapas termina siendo grande y no complejo de realizar una implementación exitosa.

6.3. Seguridad

Por el momento no existe un sistema completo que garantice la seguridad de inicio (dispositivo IoT) hasta le almacenamiento y/o procesamiento final de la información, y solo nos permite optar por tecnologías que permitan un mayor grado de seguridad; De las arquitecturas/modelos comerciales se puede identificar que la recomendación es de no conectar dispositivos de forma a Internet si este no ofrece la seguridad adecuada, y que solo se realice por medio “Gateways” que puedan proporcionar el componente de seguridad.

En este sentido podemos mencionar las existencias de marcos de trabajo como el que proporciona Cisco[75], donde se aplican sus cuatro (4) componentes básicos autorización, autenticación, visibilidad-control y políticas de red, adicionalmente las arquitecturas y/o modelos no ofrecen buenas prácticas para asegurar que los dispositivos IoT sean seguros, uno de ellos, el mas importante es la no exposición directa de un dispositivo, ya que la seguridad se vería implicada en el eslabón más débil y como se ha mencionado algunos dispositivos IoT no tienen capacidad suficiente de procesamiento para encriptar/cifrar adecuadamente la información que recolectan/reciben de forma segura.

[75] CISCO, 2017.

7. CONCLUSIONES

Se realizo un estudio monográfico con los diferentes diseños (arquitecturas) que transfieren la información usando una capa transversal de seguridad al modelo de IoT, el cual tiene un enfoque global y sin dar especificaciones en la capa uno. Ya que la capacidad de seguridad depende del hardware y software implementado.

Se analizaron diferentes arquitecturas/modelos que son comerciales y estándares internaciones de cómo implementar un sistema IoT, dentro de estas podemos mencionar IBM, Microsoft, ITU e IEEE, con los cuales se pueden a obtener el estado actual de los modelos a seguir en una implementación segura.

Se describen riegos que profundizan los problemas actuales de la seguridad de la información, en donde los problemas lógicos se convierten en físicos por la interacción con dispositivos en el mundo real. Estos por su cual añaden un riesgo adicional a los problemas actuales de seguridad.

Dentro de las diferentes modelos la seguridad va ligada a la tecnología usada, esta debe cumplir los principios de seguridad de la información con el fin de garantizar un mínimo riesgo en transferencia.

8. RECOMENDACIONES

En cuanto a dispositivos IoT, se debe usar hardware con buena capacidad de computo con el fin de que puedan procesar algoritmos criptográficos de buena seguridad con el fin de implementar buenas medidas de seguridad.

En caso de usar dispositivos hardware básico (poco poder de cálculo), sería imprescindible el uso de pasarelas o Gateway que le brinden una capa extra de seguridad a los dispositivos IoT.

BIBLIOGRAFÍA

adafruit. (2015, Noviembre 18). *DHT Humidity Sensing on Raspberry Pi or Beaglebone Black with GDocs Logging*. Retrieved from https://learn.adafruit.com/dht-humidity-sensing-on-raspberry-pi-with-gdocs-logging/overview#

adafruit. (2015, Mayo 6). *ESP8266 Temperature / Humidity Webserver*. Retrieved from https://learn.adafruit.com/esp8266-temperature-slash-humidity-webserver

Álvarez, R. (25 de Junio de 2019). *Silex, el agresivo malware que lleva más de 2000 dispositivos IoT bloqueados y que quiere poner en jaque al mundo en los próximos días*. Obtenido de XATAKA: https://www.xataka.com/seguridad/silex-agresivo-malware-que-lleva-2000-dispositivos-iot-bloqueados-que-quiere-poner-jaque-al-mundo-proximos-dias

Amazon AWS. (2017). *Internet de las cosas*. Obtenido de https://aws.amazon.com/es/iot/

Ashton, K. (2009, Junio 22). *That 'Internet of Things' Thing*. Retrieved from RFIJOURNAL: http://www.rfidjournal.com/articles/view?4986

Barranco, B. (12 de Abril de 2018). *DZone*. Recuperado el 16 de Septiembre de 2018, de https://dzone.com/articles/everything-you-need-to-know-about-iot-hardware

Barton, R., Salgueiro, G., & Hanes, D. (2017). *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things.* Cisco Press.

Chaouchi, H. (2013). *The Internet of Things: Connecting Objects.* John Wiley & Sons.

Cisco. (2014). *IoT World Forum Reference Model*. Retrieved Octubre 10, 2018, from http://cdn.iotwf.com/resources/72/IoT_Reference_Model_04_June_2014.pdf

Cisco. (2017). *Securing the Internet of Things: A Proposed Framework*. Retrieved from https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html

Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper. (16 de Diciembre de 2018). Recuperado el 2018, de CISCO:

https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html

COMPUTEX TAIPEI. (2014, Junio 9). *SlideShare*. Retrieved Noviembre 1, 2017, from 2014 IoT Forum_ IDC : https://www.slideshare.net/COMPUTEX/2014-cpx-conferenceiot-forum-idc

Espressif. (2017). *ESP8266*. Retrieved from http://espressif.com/en/products/hardware/esp8266ex/overview

Garcia, L. (26 de Abril de 2018). *The 15 best personal assistant apps*. (care.com) Recuperado el 20 de Enero de 2019, de https://www.care.com/c/stories/15112/personal-assistant-app/

Geng, H. (2017). *Internet of Things and Data Analytics Handbook.* John Wiley & Sons.

Gerber, A. (2017, Octubre 04). *Simplifique el desarrollo de sus soluciones de IoT con arquitecturas de IoT*. Retrieved Octubre 10, 2018, from https://www.ibm.com/developerworks/ssa/library/iot-lp201-iot-architectures/index.html

Greengard, S. (2015). *The Internet of Things.* MIT Press.

Hewlett Packard Enterprise. (2018). *What is Edge Computing?* Retrieved Octubre 12, 2018, from https://www.hpe.com/us/en/what-is/edge-computing.html

Hu, F. (2016). *Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations.* CRC Press.

IBM. (2018). *Internet of Things for insights from connected devices*. Retrieved Octubre 10, 2018, from https://www.ibm.com/cloud/garage/architectures/iotArchitecture/reference-architecture

IEEE. (27 de Mayo de 2015). *Towards a Definition of the Internet of Things (IoT)*. Obtenido de Define IoT: https://iot.ieee.org/definition.html

IEEE. (2017). *IoT Architecture - Internet of Things (IoT) Architecture*. Obtenido de Standards Development Working Group: https://standards.ieee.org/develop/wg/IoT_Architecture.html

imanuel. (s.f.). *Top 22 Intelligent Personal Assistants or Automated Personal Assistants*. (predictiveanalyticstoday.com) Recuperado el 15 de Febrero de 2019, de https://www.predictiveanalyticstoday.com/top-intelligent-personal-assistants-automated-personal-assistants/#content-anchor

Intel. (2015). *Intel® IoT Platform Reference Architecture*. Retrieved Octubre 10, 2018, from https://www.intel.com.au/content/www/au/en/internet-of-things/white-papers/iot-platform-reference-architecture-paper.html

International Telecommunication Union. (2012, Junio). *Internet of Things Global Standards Initiative.* Retrieved from http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

IoT Simple. (2018, Noviembre 11). *Que es Internet de las Cosas*. Retrieved from http://www.iotsimple.com/que-es-iot/

ISO/IEC. (2014, Mayo 01). *Information technology -- Advanced Message Queuing Protocol (AMQP) v1.0 specification*. Retrieved Noviembre 08, 2018, from https://www.iso.org/standard/64955.html

Jim Green, CTO Data Virtualization. (2014, Junio). *Internet of Thing World Forum*. Retrieved from IoT Reference Model: https://www.iotwf.com/resources/72

Krumm, J. (2016). *Ubiquitous Computing Fundamentals.* CRC Press.

Kumar, S. (20 de Octubre de 2017). *Make your own Google Assistant – Turn your home into Smart Home*. (icircuit.net) Recuperado el 5 de Marzo de 2019, de https://icircuit.net/make-google-assistant-turn-home-smart-home/2216

Lee, I. (2017). *The Internet of Things in the Modern Business Environment.* IGI Global.

Li Da Xu, & Li, S. (2017). *Securing the Internet of Things.* Syngress.

Lorga, M., Goren, N., Feldman, L., Barton, R., Martin, M., & Mahmoudi, C. (2018, Marzo). *Fog Computing Conceptual Model*. Retrieved Octubre 12, 2018, from https://csrc.nist.gov/publications/detail/sp/500-325/final

McEwen, A., & Cassimally, H. (2013). *Designing the Internet of Things.* John Wiley & Sons.

Mell, P., & Grance, T. (2011, Septiembre). *The NIST Definition of Cloud Computing*. Retrieved Octubre 10, 2018, from https://csrc.nist.gov/publications/detail/sp/800-145/final

Microsoft. (2018, Septiembre 26). *Microsft Azure IoT Reference Arquitecture*. Retrieved Octubre 10, 2018, from https://azure.microsoft.com/en-au/blog/azure-iot-reference-architecture-update/

Minteer, A. (2017). *Analytics for the Internet of Things (IoT).* Packt Publishing Ltd.

Oracle. (2017). *What Is an Object?* Obtenido de https://docs.oracle.com/javase/tutorial/java/concepts/object.html

Perez, X. (2017). *Using Google Assistant to control your ESP8266 devices*. (http://tinkerman.cat) Recuperado el 6 de Marzo de 2019, de http://tinkerman.cat/using-google-assistant-control-your-esp8266-devices/

Peter Saint-Andre, K. S. (2009). *XMPP: The Definitive Guide.* O'Reilly Media, Inc.

Petrov, C. (22 de Marzo de 2019). *Internet of Things Statistics 2019 [The Rise Of IoT]*. Obtenido de Internet of Things Statistics 2019 [The Rise Of IoT]: https://techjury.net/stats-about/internet-of-things-statistics/

Raspberry Pi. (2017). *Raspberry Pi*. Retrieved from https://www.raspberrypi.org/

Rodríguez Penin, A. (2012). *Sistemas SCADA.* Marcombo.

Schleicher, N. (13 de Enero de 3028). *Google Home Mini Teardown*. (ifixit.com) Recuperado el 10 de Marzo de 2019, de https://www.ifixit.com/Teardown/Google+Home+Mini+Teardown/102264

Telefónica. (22 de Agosto de 2018). *TELEFÓNICA IMPLEMENTARÁ LA PRIMERA RED EXCLUSIVA PARA IOT EN COLOMBIA*. Obtenido de telefonica.co: http://www.telefonica.co/documents/1285851/1322012/Telefonica+implementar%C3%A1+la+primera+red+para+IoT+en+Colombia/f0dbe276-fcb5-1622-67be-307f22dc1c41

Van Duren, D., & Russell, B. (2016). *Practical Internet of Things Security.* Packt Publishing.

Wilkinson, B. (2009). *Grid Computing: Techniques and Applications.* CRC Press.

Zurawski, R. (2017). *Industrial Communication Technology Handbook.* CRC Press.

INDICE

ANEXO A

ASISTENTES VIRTUALES

Un asistente virtual es un software que permite realizar tareas a un individuo mediante comandos de voz, estos también incluyen a los “chatbot” que trabajan vía comandos de texto. Actualmente existen varios asistentes virtuales, del cual listamos los principales[1]:

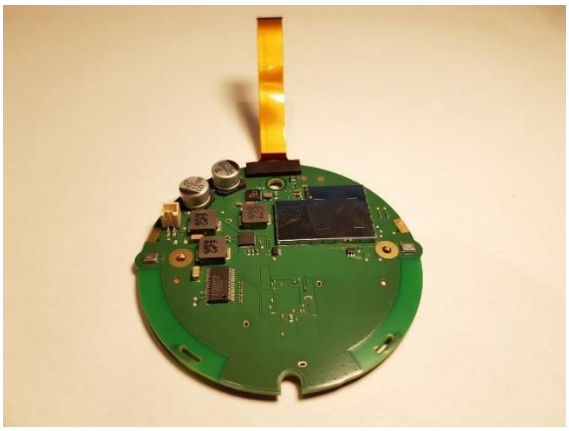
- Amazon Alexa
- Siri
- Cortana
- Google Assistant
- Bixby

De los asistentes virtuales, algunos funcionan desde el teléfono móvil, otros tienen sus propios dispositivos con los cuales trabaja, ejemplo:

- Amazon Echo
- Google Home
- Apple HomePod

Estos dispositivos terminan siendo hardware IoT como se observa con el Google Home Mini, ver imagen a continuación:

FIGURA 1 Placa de Google Home Mini



IFIXIT, Schleicher.

[1] Cinco principales obtenidos de GARCIA 2018 y IMANUEL 2019.

Con estos dispositivos como asistentes encontramos una serie de fabricantes externos de hardware y/o dispositivos IoT con el fin de crear un hogar u oficina inteligente, usando dispositivos que controlan: la temperatura, puertas, interruptores, sistemas de seguridad entre otros, y también se tiene lo entusiastas (comunidad "maker") que fabrican su propio hardware y lo enlazan con alguno de los asistentes disponibles, para este caso los dos más usados son:

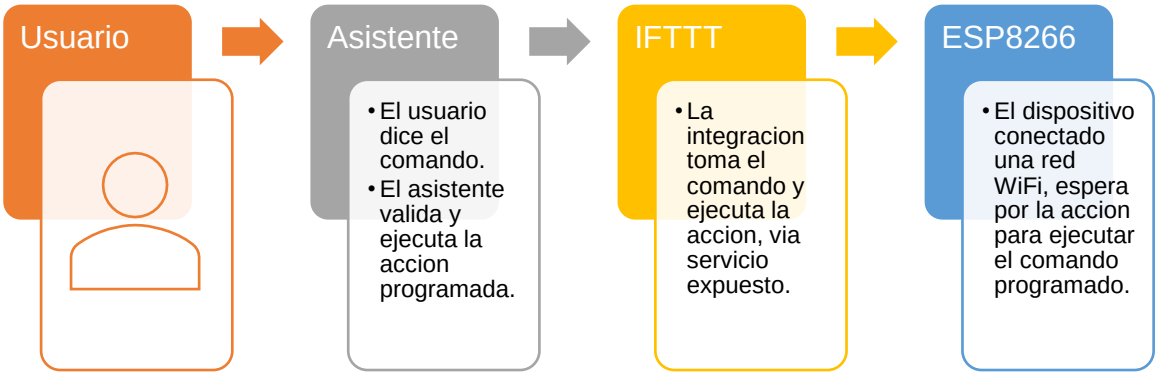
- Amazon Echo, con Alexa.
- Google Home, con Asistente de Google.

Los fabricantes como Philips, hue, wemo, TP-Link entre otros, proporcionan su propia infraestructura para trabajar en conjunto con algunos de los asistentes, pero los que hacen sus propios productos terminan construyendo sus productos sin tener en cuenta el tema de la seguridad, un ejemplo, es la creación de toma eléctrico y/o interruptor eléctrico que permite encender o apagar aparatos eléctricos que no cuentan con una conexión WiFi, para esto se requiere los siguientes materiales[2][3][4]:

- Un Asistente (sea de Google o Amazon).
- Esp8266
- Servicio IFTTT[5]
- Conexión a internet
- Un poco de programación.

En la siguiente imagen se puede observar cómo sería la interacción entre ellos:

FIGURA 2 Diagrama de Interacción con el dispositivo.



Autor, interacción de los tres componentes.

[2] Ejemplo para comunicar la internet con el dispositivo, PEREZ, 2017.
[3] Ejemplo realizando una conexión inversa para exponer un servicio http, KUMAR 2017.
[4] Ejemplo de abrir un puerto del router/moden para realizar conexión, VOLDERS, 2017.
[5] Servicio para ejecutar eventos entre otros servicios "If This Then That" que en español seria "Si ocurre esto, entonces has esto", https://ifttt.com/.

El riesgo de seguridad está en la comunicación IFTTT y ESP8266, en el cual se puede de hacer de dos formas inseguras:

- Abriendo el puerto del router/moden.
- Exponiendo el servicio de conexión inversa usando un servicio como ngrok[6].

Al realizar esta configuración y no poner un firewall de intermedio, se está exponiendo a que un atacante infiltre la red del hogar u oficina, con esta forma, se estaría incurriendo en una mala práctica, una forma segura de realizarlo es usando un intermediario que evite que abra o se realicen una conexión inversa, por ejemplo, un servicio MQTT[7]. De esta forma el dispositivo ESP8266 estaría censando la cola con el fin de ejecutar la acción programada.

Con el ejemplo anterior se está mostrando una vulnerabilidad de los dispositivos IoT que se fabrican de forma “cacera” y/o de fabricantes que no tienen buenas prácticas a la hora de integrarse con los asistentes personales virtuales.

[6] Servicio de túnel con el cual se expone una página web a la internet, https://ngrok.com/
[7] Ejemplo usando una forma segura de realizar la integración, SAEED 2018.

BIBLIOGRAFIA

Garcia, L. (26 de Abril de 2018). *The 15 best personal assistant apps*. (care.com) Recuperado el 20 de Enero de 2019, de https://www.care.com/c/stories/15112/personal-assistant-app/

imanuel. (s.f.). *Top 22 Intelligent Personal Assistants or Automated Personal Assistants*. (predictiveanalyticstoday.com) Recuperado el 15 de Febrero de 2019, de https://www.predictiveanalyticstoday.com/top-intelligent-personal-assistants-automated-personal-assistants/#content-anchor

Kumar, S. (20 de Octubre de 2017). *Make your own Google Assistant – Turn your home into Smart Home*. (icircuit.net) Recuperado el 5 de Marzo de 2019, de https://icircuit.net/make-google-assistant-turn-home-smart-home/2216

Perez, X. (2017). *Using Google Assistant to control your ESP8266 devices*. (http://tinkerman.cat) Recuperado el 6 de Marzo de 2019, de http://tinkerman.cat/using-google-assistant-control-your-esp8266-devices/

SAEED, K. (2018). *Controlling IoT devices with Google Assistant*. (diygeeks.org) Recuperado el 10 de Marzo de 2019, de https://diygeeks.org/learn/controlling-iot-devices-with-google-assistant/

Schleicher, N. (13 de Enero de 3028). *Google Home Mini Teardown*. (ifixit.com) Recuperado el 10 de Marzo de 2019, de https://www.ifixit.com/Teardown/Google+Home+Mini+Teardown/102264

Volders, L. (20 de MAyo de 2017). *Google Home and the ESP8266*. (http://lucstechblog.blogspot.com) Recuperado el 07 de Marzo de 2019, de http://lucstechblog.blogspot.com/2017/05/google-home-and-esp8266.html

ありがとう

RESUMEN ANALÍTICO DE EDUCACIÓN - RAE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

FECHA			Septiembre 11 de 2019				
TITULO			Arquitecturas de referencia para IoT con transferencia segura de información				
AUTOR (Libro, Monografía)			Andrés Vélez Pérez				
AUTOR DEL RAE			Andrés Vélez Pérez				
EDICIÓN			UNAD				
DIRECTOR (ES)/ ASESOR(ES)			MARTIN CAMILO CANCELADO RUIZ				
AÑO ELABORACIÓN			2018				
DESCRIPCIÓN			Monográfia sobre diseños (arquitecturas) de transferencia de información segura en IoT, mediante el análisis de las diferentes propuestas que existen para la transferencia de datos.				
PAGINAS	**74**	**TABLAS**	**3**	**FIGURAS**	**28**	**ANEXOS**	**1**

CONTENIDO

PALABRAS CLAVES

Internet de las Cosas, Internet of Things, Arquitectura, seguridad de la información.

FORMULACIÓN DEL PROBLEMA

El Internet de las Cosas (IoT, del inglés Internet of Things), consiste en una red interconectada de dispositivos (cosas u objetos), que son sensores, los cuales tienen la capacidad de generar y transmitir información hacia la nube (internet) o servidor, esta información que es transmitida puede estar expuesta a riesgos que degradan la información con consecuencias inesperadas para los servicios que estos están monitoreando.

En este sentido se ha vuelto critico la seguridad de la data transmitida por estos dispositivos ya que transfieren la información de forma inalámbrica (WiFi, Bluetooh, 3G, 4G), algunos dispositivos no tienen la suficiente capacidad de procesamiento para generar canales seguros (encriptación de datos) entre el dispositivo inicial y su destino final, es por esto que se busca los mejores estándares/modelos con el fin de divulgar y cerrar la brecha de conocimiento ya que se esperan 500 billones de dispositivos para el 2030 , en el 2017 fueron 17 billones, y los riesgos de dispositivos comprometidos se cuentan por millares . En Colombia el proveedor Telefónica tiene un total 600.000 soluciones IoT con 14.000 clientes, el cual corresponde al 60% del mercado empresarial, es decir, que en Colombia supera el millón de dispositivos IoT conectados.

OBJETIVOS

Objetivo general:

Realizar un estudio monográfico del diseño (arquitectura) u transferencia de información segura en IoT, mediante el análisis de las diferentes propuestas que existen para la transferencia de datos con enfoque en la capa uno.

Objetivos específicos:

1. Analizar los principales estándares en arquitecturas de las redes IoT.
2. Describir los riesgos a los cuales está expuesto la transferencia de información de los dispositivos IoT con conectividad WiFi en la capa uno.
3. Analizar los métodos seguros actuales de transferencia de Información en IoT.
4. Proponer el diseño (arquitectura) transferencia segura de información en IoT en la capa uno.

CONTENIDO

Definición y origen de «Internet of Things».

Descripción de las diferentes arquitecturas en «Internet of Things», propuestas por organismos de estandarización internacionales y autores que proponen otros diseños con un componente transversal de seguridad.

- Dispositivos
- Protocolos de Comunicación
- Procesamiento de Datos
- Seguridad
- Arquitecturas
    - Modelo ITU
    - Modelo IEEE
    - Modelo de Barton, Salgueiro, & Hanes
    - Modelo IoTWF
    - Intel IoT Platform Refrence Arquitecture
    - IoT Simple
    - Arquitectura de Referencia de IoT de IBM
    - Azure IoT Reference Architecture

METODOLOGIA DE INVESTIGACION

Para realizar el estudio se opta por una búsqueda sistemática de bibliografía que evidencie el uso de Arquitecturas de Referencia del Internet de las Cosas con énfasis en la transferencia segura de información.

CONCLUSIONES

Se realizo un estudio monográfico con los diferentes diseños (arquitecturas) que transfieren la información usando una capa transversal de seguridad al modelo de IoT, el cual tiene un enfoque global y sin dar especificaciones en la capa uno. Ya que la capacidad de seguridad depende del hardware y software implementado.

Se analizaron diferentes arquitecturas/modelos que son comerciales y estándares internaciones de cómo implementar un sistema IoT, dentro de estas podemos mencionar IBM, Microsoft, ITU e IEEE, con los cuales se pueden a obtener el estado actual de los modelos a seguir en una implementación segura.

Se describen riegos que profundizan los problemas actuales de la seguridad de la información, en donde los problemas lógicos se convierten en físicos por la interacción con dispositivos en el mundo real. Estos por su cual añaden un riesgo adicional a los problemas actuales de seguridad.

Dentro de las diferentes modelos la seguridad va ligada a la tecnología usada, esta debe cumplir los principios de seguridad de la información con el fin de garantizar un mínimo riesgo en transferencia.

RECOMENDACIONES

Definiciones:
Se expusieron ocho (8) modelos de arquitecturas de IoT, en que tres modelos son genéricos y los otros corresponden a la oferta de IoT como un servicio, donde especifican que algunos componentes pueden ser genéricos y otros de su propia marca. Todos ofrecen una seguridad inherente a la tecnología usada.
Hay un punto en común en la mayoría de los modelos, es que no exponen de forma directa los dispositivos IoT (al menos que no sea móvil), y que exista un previo procesamiento antes de que la data se almacene (en la nube).

Modelos Genéricos:

- Modelo ITU
- Modelo IEEE
- Modelo de Barton, Salgueiro, & Hanes

Modelos Comerciales:

- Modelo IoTWF
- Intel IoT Platform Refrence Arquitecture
- IoT Simple
- Arquitectura de Referencia de IoT de IBM
- Azure IoT Reference Architecture

El modelo IoTWF actúa como un modelo genérico su enfoque es comercial, ya que toma de la industria su modelo con el fin de mostrar el estado actual de la industria y no un modelo general para su adopción.
El Modelo IEEE es un borrador que no ha sido publicado como un estándar y sigue en proceso de refinamiento.
En la siguiente tabla se describen algunas características de los modelos y/o arquitectura:

Tabla de comparación entre modelos de IoT

Modelo	Numero de Capas	Capa de Seguridad Transversal	Cloud Propia	Usa productos propios.	Edge
ITU	4	SI	NO	NO	NO ESPECIFICA
IEEE	3	SI	NO	NO	NO ESPECIFICA

Barton, Salgueiro, & Hanes	3	SI	NO	NO	SI
IoTWF	7	SI	NO	PARTNER	SI
Intel	6	SI	SI	SI	SI
IoT Simple	5	SI	SI	SI	PARCIAL
IBM	3	SI	SI	SI	SI
Azure	3	SI	SI	SI	SI

Autor, diferencia en características.

Todos los modelos y/o arquitecturas garantizan las siguientes características:

- Seguridad.
- Interoperatividad:
  - Entre Dispositivos.
  - Entre Componentes de Software
- Análisis de datos.
- Almacenamiento de información.
- Flexibilidad
- Escalabilidad
- Control de dispositivos.

Arquitecturas recomendadas:

Para determinar las arquitecturas recomendadas validaremos los siguientes puntos:

- [1] Capa transversal de seguridad.
- [2]Administrable.
- [3]Interoperable
- [4]Heterogéneo.
- [5]Independiente de un fabricante.
- [6]Compatible con proveedores de plataforma.

Selección del Modelo de Referencia

Modelo	1	2	3	4	5	6
ITU	SI	SI	SI	SI	SI	SI
IEEE	SI	SI	SI	SI	SI	SI
Barton, Salgueiro, & Hanes	SI	SI	SI	SI	SI	SI
IoTWF	SI	SI	SI	PARCIAL	PARCIAL	PARCIAL
Intel	SI	SI	PARCIAL	PARCIAL	NO	PARCIAL
IoT Simple	SI	SI	PARCIAL	PARCIAL	PARCIAL	PARCIAL
IBM	SI	SI	PARCIAL	PARCIAL	NO	PARCIAL
Azure	SI	SI	PARCIAL	PARCIAL	NO	PARCIAL

Autor, selección del modelo de referencia.

Analizando los anteriores parámetros podemos inferir de la Tabla 3, que la condición «Independiente de plataforma» deja por fuera a los modelos comerciales, es decir, no implementar una suite completa de algún fabricante ya que puede que las necesidades no sean la esperadas, otro punto negativo son

los esfuerzos en crear integraciones para hacer que otros sistemas funcionen con un modelo propietario.
EL modelo de la IEEE sigue siendo un borrador y no un estándar aprobado, así que puede tener variaciones y definiciones sobre sus capas, aunque podemos tomar características para mejorar nuestra implementación de una arquitectura IoT.
El modelo explicado en el libro Barton, Salgueiro, & Hanes, no intenta ser una arquitectura de referencia, pero explica capa por capa que es lo que debería de tener, aunque su modelo de tres (3) capas explica es similar a otros da una visión entera de este tipo de arquitecturas.
De las arquitecturas se pueden recomendar dos modelos:
1.- Modelo ITU
2.- Modelo de Barton, Salgueiro, & Hanes

Aunque estos modelos se ven a simple vista simplificados, la estructura de las subcapas termina siendo grande y no complejo de realizar una implementación exitosa.

Seguridad:
Por el momento no existe un sistema completo que garantice la seguridad de inicio (dispositivo IoT) hasta le almacenamiento y/o procesamiento final de la información, y solo nos permite optar por tecnologías que permitan un mayor grado de seguridad; De las arquitecturas/modelos comerciales se puede identificar que la recomendación es de no conectar dispositivos de forma a Internet si este no ofrece la seguridad adecuada, y que solo se realice por medio "Gateways" que puedan proporcionar el componente de seguridad.
En este sentido podemos mencionar las existencias de marcos de trabajo como el que proporciona Cisco, donde se aplican sus cuatro (4) componentes básicos autorización, autenticación, visibilidad-control y políticas de red, adicionalmente las arquitecturas y/o modelos no ofrecen buenas prácticas para asegurar que los dispositivos IoT sean seguros, uno de ellos, el más importante es la no exposición directa de un dispositivo, ya que la seguridad se vería implicada en el eslabón más débil y como se ha mencionado algunos dispositivos IoT no tienen capacidad suficiente de procesamiento para encriptar/cifrar adecuadamente la información que recolectan/reciben de forma segura.

Recomendaciones finales:
En cuanto a dispositivos IoT, se debe usar hardware con buena capacidad de computo con el fin de que puedan procesar algoritmos criptográficos de buena seguridad con el fin de implementar buenas medidas de seguridad.

En caso de usar dispositivos hardware básico (poco poder de cálculo), sería imprescindible el uso de pasarelas o Gateway que le brinden una capa extra de seguridad a los dispositivos IoT.

FUENTES BIBLIOGRAFICAS

adafruit. (2015, Noviembre 18). DHT Humidity Sensing on Raspberry Pi or Beaglebone Black with GDocs Logging. Retrieved from https://learn.adafruit.com/dht-humidity-sensing-on-raspberry-pi-with-gdocs-logging/overview#
adafruit. (2015, Mayo 6). ESP8266 Temperature / Humidity Webserver. Retrieved from https://learn.adafruit.com/esp8266-temperature-slash-humidity-webserver
Álvarez, R. (25 de Junio de 2019). Silex, el agresivo malware que lleva más de 2000 dispositivos IoT bloqueados y que quiere poner en jaque al mundo en los próximos días. Obtenido de XATAKA: https://www.xataka.com/seguridad/silex-agresivo-malware-que-lleva-2000-dispositivos-iot-bloqueados-que-quiere-poner-jaque-al-mundo-proximos-dias
Amazon AWS. (2017). Internet de las cosas. Obtenido de https://aws.amazon.com/es/iot/
Ashton, K. (2009, Junio 22). That 'Internet of Things' Thing. Retrieved from RFIJOURNAL: http://www.rfidjournal.com/articles/view?4986
Barranco, B. (12 de Abril de 2018). DZone. Recuperado el 16 de Septiembre de 2018, de https://dzone.com/articles/everything-you-need-to-know-about-iot-hardware
Barton, R., Salgueiro, G., & Hanes, D. (2017). IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things. Cisco Press.
Chaouchi, H. (2013). The Internet of Things: Connecting Objects. John Wiley & Sons.
Cisco. (2014). IoT World Forum Reference Model. Retrieved Octubre 10, 2018, from http://cdn.iotwf.com/resources/72/IoT_Reference_Model_04_June_2014.pdf
Cisco. (2017). Securing the Internet of Things: A Proposed Framework. Retrieved from https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html
Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper. (16 de Diciembre de 2018). Recuperado el 2018, de CISCO: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html
COMPUTEX TAIPEI. (2014, Junio 9). SlideShare. Retrieved Noviembre 1, 2017, from 2014 IoT Forum_ IDC : https://www.slideshare.net/COMPUTEX/2014-cpx-conferenceiot-forum-idc
Espressif. (2017). ESP8266. Retrieved from http://espressif.com/en/products/hardware/esp8266ex/overview
Garcia, L. (26 de Abril de 2018). The 15 best personal assistant apps. (care.com) Recuperado el 20 de Enero de 2019, de https://www.care.com/c/stories/15112/personal-assistant-app/
Geng, H. (2017). Internet of Things and Data Analytics Handbook. John Wiley & Sons.
Gerber, A. (2017, Octubre 04). Simplifique el desarrollo de sus soluciones de IoT con arquitecturas de IoT. Retrieved Octubre 10, 2018, from

https://www.ibm.com/developerworks/ssa/library/iot-lp201-iot-architectures/index.html
Greengard, S. (2015). The Internet of Things. MIT Press.
Hewlett Packard Enterprise. (2018). What is Edge Computing? Retrieved Octubre 12, 2018, from https://www.hpe.com/us/en/what-is/edge-computing.html
Hu, F. (2016). Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations. CRC Press.
IBM. (2018). Internet of Things for insights from connected devices. Retrieved Octubre 10, 2018, from https://www.ibm.com/cloud/garage/architectures/iotArchitecture/reference-architecture
IEEE. (27 de Mayo de 2015). Towards a Definition of the Internet of Things (IoT). Obtenido de Define IoT: https://iot.ieee.org/definition.html
IEEE. (2017). IoT Architecture - Internet of Things (IoT) Architecture. Obtenido de Standards Development Working Group: https://standards.ieee.org/develop/wg/IoT_Architecture.html
imanuel. (s.f.). Top 22 Intelligent Personal Assistants or Automated Personal Assistants. (predictiveanalyticstoday.com) Recuperado el 15 de Febrero de 2019, de https://www.predictiveanalyticstoday.com/top-intelligent-personal-assistants-automated-personal-assistants/#content-anchor
Intel. (2015). Intel® IoT Platform Reference Architecture. Retrieved Octubre 10, 2018, from https://www.intel.com.au/content/www/au/en/internet-of-things/white-papers/iot-platform-reference-architecture-paper.html
International Telecommunication Union. (2012, Junio). Internet of Things Global Standards Initiative. Retrieved from http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx
IoT Simple. (2018, Noviembre 11). Que es Internet de las Cosas. Retrieved from http://www.iotsimple.com/que-es-iot/
ISO/IEC. (2014, Mayo 01). Information technology -- Advanced Message Queuing Protocol (AMQP) v1.0 specification. Retrieved Noviembre 08, 2018, from https://www.iso.org/standard/64955.html
Jim Green, CTO Data Virtualization. (2014, Junio). Internet of Thing World Forum. Retrieved from IoT Reference Model: https://www.iotwf.com/resources/72
Krumm, J. (2016). Ubiquitous Computing Fundamentals. CRC Press.
Kumar, S. (20 de Octubre de 2017). Make your own Google Assistant – Turn your home into Smart Home. (icircuit.net) Recuperado el 5 de Marzo de 2019, de https://icircuit.net/make-google-assistant-turn-home-smart-home/2216
Lee, I. (2017). The Internet of Things in the Modern Business Environment. IGI Global.
Li Da Xu, & Li, S. (2017). Securing the Internet of Things. Syngress.
Lorga, M., Goren, N., Feldman, L., Barton, R., Martin, M., & Mahmoudi, C. (2018, Marzo). Fog Computing Conceptual Model. Retrieved Octubre 12, 2018, from https://csrc.nist.gov/publications/detail/sp/500-325/final
McEwen, A., & Cassimally, H. (2013). Designing the Internet of Things. John Wiley & Sons.

Mell, P., & Grance, T. (2011, Septiembre). The NIST Definition of Cloud Computing. Retrieved Octubre 10, 2018, from https://csrc.nist.gov/publications/detail/sp/800-145/final
Microsoft. (2018, Septiembre 26). Microsft Azure IoT Reference Arquitecture. Retrieved Octubre 10, 2018, from https://azure.microsoft.com/en-au/blog/azure-iot-reference-architecture-update/
Minteer, A. (2017). Analytics for the Internet of Things (IoT). Packt Publishing Ltd.
Oracle. (2017). What Is an Object? Obtenido de https://docs.oracle.com/javase/tutorial/java/concepts/object.html
Perez, X. (2017). Using Google Assistant to control your ESP8266 devices. (http://tinkerman.cat) Recuperado el 6 de Marzo de 2019, de http://tinkerman.cat/using-google-assistant-control-your-esp8266-devices/
Peter Saint-Andre, K. S. (2009). XMPP: The Definitive Guide. O'Reilly Media, Inc.
Petrov, C. (22 de Marzo de 2019). Internet of Things Statistics 2019 [The Rise Of IoT]. Obtenido de Internet of Things Statistics 2019 [The Rise Of IoT]: https://techjury.net/stats-about/internet-of-things-statistics/
Raspberry Pi. (2017). Raspberry Pi. Retrieved from https://www.raspberrypi.org/
Rodríguez Penin, A. (2012). Sistemas SCADA. Marcombo.
Schleicher, N. (13 de Enero de 3028). Google Home Mini Teardown. (ifixit.com) Recuperado el 10 de Marzo de 2019, de https://www.ifixit.com/Teardown/Google+Home+Mini+Teardown/102264
Telefónica. (22 de Agosto de 2018). TELEFÓNICA IMPLEMENTARÁ LA PRIMERA RED EXCLUSIVA PARA IOT EN COLOMBIA. Obtenido de telefonica.co: http://www.telefonica.co/documents/1285851/1322012/Telefonica+implementar%C3%A1+la+primera+red+para+IoT+en+Colombia/f0dbe276-fcb5-1622-67be-307f22dc1c41
Van Duren, D., & Russell, B. (2016). Practical Internet of Things Security. Packt Publishing.
Wilkinson, B. (2009). Grid Computing: Techniques and Applications. CRC Press.
Zurawski, R. (2017). Industrial Communication Technology Handbook. CRC Press.