Dom. Cien., ISSN: 2477-8818
Vol. 6, núm. 3, julio-septiembre 2020, pp. 342-363

DOI: http://dx.doi.org/10.23857/dc.v6i3.1288

Ciencias de la Tecnología

Artículo de investigación

Análisis de las estrategias aplicadas en el desarrollo de sistemas domóticos de seguridad

Analysis of the strategies applied in the development of home automation security systems

Análise das estratégias aplicadas no desenvolvimento de sistemas de segurança de automação residencial

Lester Geovanny Ojeda-Crespo [I]
lgojedac@hotmail.com
https://orcid.org/0000-0001-7353-0238

Javier Bernardo Cabrera-Mejía [II]
jcabreram@ucacue.edu.ec
https://orcid.org/0000-0003-2027-0211

***Recibido:** 26 de mayo de 2020 ***Aceptado:** 29 de junio de 2020 *** Publicado:** 18 de julio de 2020

I. Estudiante de la Maestría en Tecnologías de la Información, Jefatura de Posgrados, Universidad Católica de Cuenca, Cuenca, Ecuador.
II. Docente Investigador de la Jefatura de Posgrados, Universidad Católica de Cuenca. Cuenca, Ecuador.

Resumen

En la sociedad actual, el manejo de la información tiene una importancia muy significativa. La generación, comunicación, transformación y almacenamiento de los datos forma parte esencial de la vida moderna. En este sentido; conceptos como el de Internet de las Cosas (IoT), cobra una importancia notable en muchos aspectos y también en la domótica.

La existencia de múltiples dispositivos inteligentes en el ámbito del hogar, hace de las aplicaciones domóticas un campo de prueba excelente para estos nuevos conceptos. En este trabajo nos proponemos el análisis del protocolo MQTT para brindar una solución basada en eventos y escalable.

La solución brindada utiliza las ventajas del MQTT como protocolo flexible y sencillo, que permite coordinar el funcionamiento de diferentes dispositivos inteligentes.

El método de investigación aplicado es bibliográfico y descriptivo, el mismo que examina el enfoque de la domótica y los organismos de normalización inmersos, los cuales proporcionan la documentación fiable para la implementación de sistemas robustos; por lo cual, se enfatiza en normativas proyectadas a solventar las dificultades de gestión y seguridad de los sistemas domóticos, como el protocolo de comunicación MQTT que permite el control domótico, implementando recursos limitados con baja sobrecarga adaptado para nodos restringidos. Es necesario la implementación de las tecnologías basadas en las buenas prácticas y estándares internacionales que garanticen la integridad de sus servicios.

Palabras claves: Estrategias de seguridad; gobierno de TI; MQTT; sistemas domóticos.

Abstract

In today's society, the handling of information has a very significant importance. The generation, communication, transformation and storage of data is an essential part of modern life. In this sense; concepts such as the Internet of Things (IoT), takes on considerable importance in many aspects and also in home automation.

The existence of multiple smart devices in the home environment makes home automation applications an excellent testing ground for these new concepts. In this work we propose the analysis of the MQTT protocol to provide a scalable, event-based solution.

The solution provided uses the advantages of the MQTT as a flexible and simple protocol, which allows the operation of different smart devices to be coordinated.

The applied research method is bibliographic and descriptive, the same that examines the approach of home automation and immersed standardization organisms, which provide reliable documentation for the implementation of robust systems; therefore, it is emphasized in regulations designed to solve the management and security difficulties of home automation systems, such as the MQTT communication protocol that allows home automation control, implementing limited resources with low overload adapted for restricted nodes. The implementation of technologies based on good practices and international standards that guarantee the integrity of its services is necessary.

Keywords: Security strategies; IT governance; MQTT; home automation systems.

Resumo

Na sociedade de hoje, o manuseio da informação tem uma importância muito significativa. A geração, comunicação, transformação e armazenamento de dados é uma parte essencial da vida moderna. Neste sentido; conceitos como a Internet das Coisas (IoT), assumem uma importância considerável em muitos aspectos e também na automação residencial.

A existência de vários dispositivos inteligentes no ambiente doméstico torna os aplicativos de automação residencial um excelente campo de teste para esses novos conceitos. Neste trabalho, propomos a análise do protocolo MQTT para fornecer uma solução escalável baseada em eventos. A solução fornecida utiliza as vantagens do MQTT como um protocolo flexível e simples, que permite coordenar a operação de diferentes dispositivos inteligentes.

O método de pesquisa aplicada é bibliográfico e descritivo, o mesmo que examina a abordagem de automação residencial e organismos de padronização imersos, que fornecem documentação confiável para a implementação de sistemas robustos; portanto, é enfatizado em regulamentos projetados para resolver as dificuldades de gerenciamento e segurança dos sistemas de automação residencial, como o protocolo de comunicação MQTT que permite o controle da automação residencial, implementando recursos limitados com baixa sobrecarga adaptada para nós restritos. É necessária a implementação de tecnologias baseadas em boas práticas e padrões internacionais que garantam a integridade de seus serviços.

Palavras-chave: Estratégias de segurança; Governança de TI; MQTT; sistemas de automação residencial.

Introducción

En los últimos años hay ciertos factores que están ganando importancia dentro de la sociedad tales como la información, la comunicación, la instantaneidad y la eficiencia, por poner algunos ejemplos. Gran parte de la culpa la tiene el avance de la tecnología, y en concreto las Tecnologías de la Información y la Comunicación (TIC). Es por eso por lo que el Internet de las Cosas (IoT) esté ganando protagonismo, y más aun dentro del concepto de domótica.

El internet de las cosas (IoT) es un paradigma basado en la interconexión de dispositivos, a los cuales se les proporciona una conexión a internet para que puedan interaccionar entre ellos. Estos dispositivos pueden ser sensores, actuadores, objetos cotidianos, etc. En definitiva, cualquier cosa podría adquirir una conexión a internet y establecer una comunicación que nos permita enviar y recibir información extrayendo un beneficio de ello.

En la línea de las nuevas necesidades en las aplicaciones informáticas y gracias a que los avances tecnológicos lo permiten, toma importancia el manifiesto de Sistemas Reactivos, una propuesta para satisfacer la nueva filosofía de los sistemas, que define cuatro aspectos clave que deben poseer estos: responsabilidad, resiliencia, elasticidad y que sean orientados a mensajes. Estos sistemas tienen bajos tiempos de respuesta lo que permite que los errores se detecten rápidamente y al ser resilientes, pueden seguir siendo responsivos incluso después de suceder el fallo. Los fallos se aíslan en el componente en el que sucede, permitiendo que si ocurre un fallo se pueda recuperar sin comprometer al sistema como un todo. Al ser elásticos son responsivos sin depender de la carga del sistema, adaptando los recursos para llevar a cabo la tarea. En cierto modo, un agente escalable es a su vez elástico, ya que al crecer sus prestaciones adapta los recursos para hacer frente a esa mayor demanda. Son también orientados a mensajes, siendo estos asíncronos, lo que permite que haya un bajo acoplamiento y que la comunicación sea no-bloqueante, es decir, los dispositivos consumen los recursos solo cuando estos están activos.

Tiempo atrás, las aplicaciones eran frágiles, síncronas y estaban fuertemente acopladas, lo que derivaba en sistemas de gran complejidad. Esto era debido a que dichas aplicaciones eran construidas en base a la tecnología disponible, donde la comunicación entre los distintos elementos

o agentes era cableada y requería diseñar muy bien de antemano los sistemas y prever las posibles modificaciones o ampliaciones de este, y en consecuencia las comunicaciones son rígidas. Sin embargo, con el avance de la tecnología y con ello la mejora de la comunicación inalámbrica y la aparición del Wifi, se consigue una menor rigidez en el ámbito físico. Además, permite una mayor dispersión geográfica de los dispositivos y poder conectar elementos que hace años sería impensable; es decir, dotar de conexión a internet a las cosas (IoT), teniendo una mayor posibilidad de interacción entre agentes, obteniendo una mayor escalabilidad y mejor acoplamiento. Es por todo esto que es necesario que existan protocolos de comunicación que se adapten a las nuevas exigencias.

En este contexto han surgido una serie de protocolos de comunicación que dan soporte a las necesidades anteriormente descritas y encajan en el paradigma del IoT, tales como Advanced Message Queuing Protocol (AMQP), Constrained Application Protocol (CoAP), Data Distribution Service (DDS), Message Queue Telemetry Transport (MQTT) entre otros. En la Tabla 1 se pueden apreciar las principales diferencias entre los mencionados protocolos, cortesía del instituto nacional de ciberseguridad.

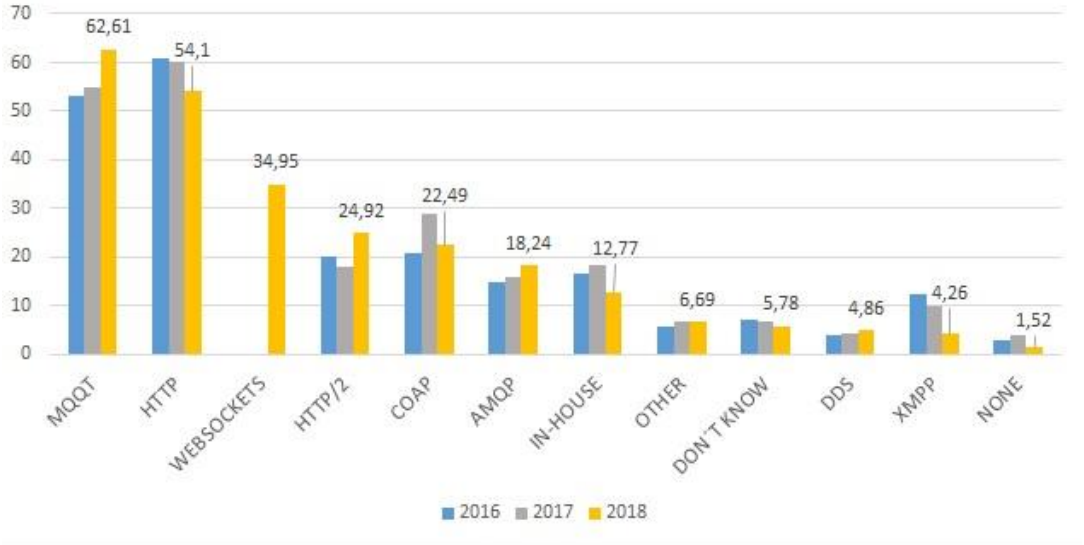
Tabla 1. Comparación de protocolos IoT

	Transporte	**Modelo**	**Ámbito de aplicación**	**Conocimiento del contenido**	**Datos principales**	**Seguridad**	**Prioridad de los datos**	**Tolerancia a fallos**
AMQP	TCP/IP	Intercambio de mensajes punto a punto	D2D D2C C2C	Ninguno	Codificados	TLS	Ninguno	Específica de la implementación
CoAP	UDP/IP	Petición/Respuesta (REST)	D2D	Ninguno	Codificados	DTLS	Ninguno	Descentralizado
DDS	UDP/IP (unicast + mcast) TCP/IP	Publicación/Suscripción Petición/Respuesta	D2D D2C C2C	Enrutamiento basado en el contenido, consultas	Declarados codificados	TLS, DTLS, DDS	Prioridades de transporte	Descentralizado
MQQT	TCP/IP	Publicación/Suscripción	D2C	Ninguno	No definidos	TLS	ninguno	El nodo central (broker) es el punto único de fallo (SPoF)

MQTT es un protocolo de mensajería asíncrona que disocia al emisor y al receptor tanto en espacio como en tiempo, y a pesar de que su nombre diga “queue” no tiene nada que ver con colas de mensajería que tradicionalmente se conocen en informática, aunque sí que es posible generar colas de mensajes con otros mecanismos que se verán más adelante en profundidad. Utiliza un modelo de publicación y suscripción, el cual es no-bloqueante, lo que permite que no sea necesaria una red muy fiable. Es un protocolo liviano y flexible, lo que hace que pueda implementarse en dispositivos con recursos limitados y se adapte a situaciones con diferente demanda de recursos. La comunicación es posible gracias a un intermediario de mensajes entre los distintos clientes, que puede ser cualquier cosa capaz de enviar o recibir mensajes. El cliente publica un mensaje en un tema o topic, que se lo envía al intermediario, o también llamado broker, el cual redirige este mensaje al cliente o clientes que estén suscritos a ese topic. Puesto que los mensajes están organizados por temas proporciona una jerarquía a la estructura del sistema.

Se aprecian concordancias entre el protocolo MQTT y el manifiesto de los Sistemas Reactivos, y a su vez dicho protocolo encaja muy bien con el paradigma del IoT. Es por esto por lo que es el elegido para el desarrollo del presente trabajo. Igualmente, el protocolo MQTT está cogiendo peso últimamente como se puede observar en la figura 1, creciendo su uso frente a otros protocolos.

Figura 1. Tendencias de uso de protocolos de IoT



Cuando los procedimientos enfocados en garantizar la seguridad carecen, se obtienen productos insolventes ante situaciones o acciones que emergen estabilidad y protección de los datos. Para lo cual, es preciso disponer de factores de seguridad basados en buenas prácticas y normativas que se involucren en el desarrollo de sistemas para resguardar la integridad, confiabilidad y disponibilidad de los servicios. La necesidad de gestionar los procesos y dar un valor al desarrollo de sistemas domóticos, tienen una implicación al cumplimiento de los objetivos estratégicos. Para lo cual el presente estudio, está centrado en analizar las estrategias de seguridad que se involucran en el desarrollo de los sistemas domóticos para potenciar el bienestar humano, enfatizando en el protocolo.

Message Queue Server Telemetry Transport (MQTT) es una arquitectura de publicación y suscripción desarrollada principalmente para conectar el ancho de banda y los dispositivos con limitaciones de energía a través de redes. MQTT tiene dos componentes: un intermediario MQTT y un cliente MQTT. Un intermediario MQTT es un punto central de comunicación y distribuye todos los mensajes entre los clientes, un cliente MQTT es un dispositivo (por ejemplo, un ordenador o un teléfono móvil) que se conecta al intermediario.

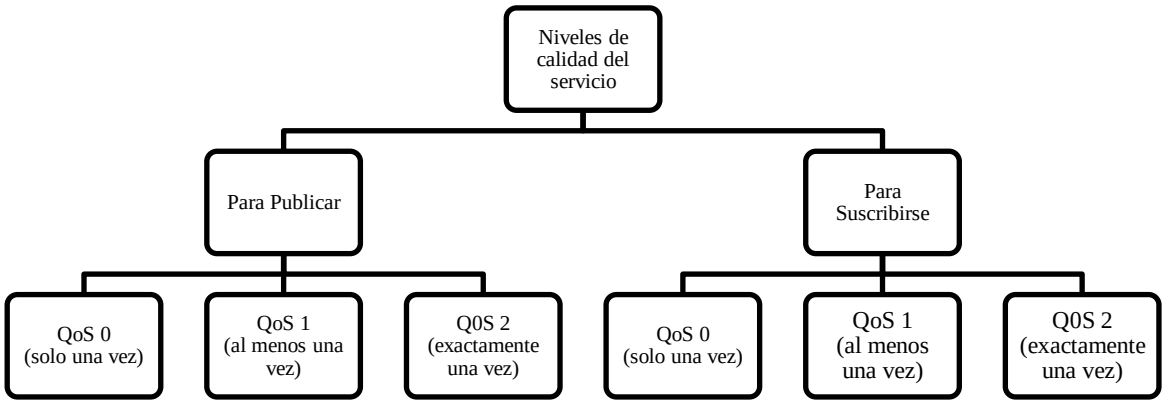
Un cliente que envía mensajes al intermediario es un editor, y si recibe mensajes del intermediario es un suscriptor. Para recibir un mensaje, el cliente debe suscribirse al tema de ese mensaje.

Puede publicar y suscribirse a mensajes MQTT mediante bloques MQTT Publish y MQTT Subscribe. Estos bloques admiten MQTT solo a través de sockets TCP/IP.

Niveles de QoS en MQTT

Calidad de servicio (QoS) define la fiabilidad del proceso de entrega de mensajes en MQTT. MQTT proporciona tres niveles de QoS para la entrega de mensajes: QoS 0, QoS 1 y QoS 2. Puede tener diferentes niveles de QoS para publicar y para suscribirse a mensajes. Es posible que el intermediario MQTT que está utilizando no admita los tres niveles de QoS. Por ejemplo, ThingSpeak MQTT solo admite QoS 0.

Figura 2. Niveles de QoS en MQTT

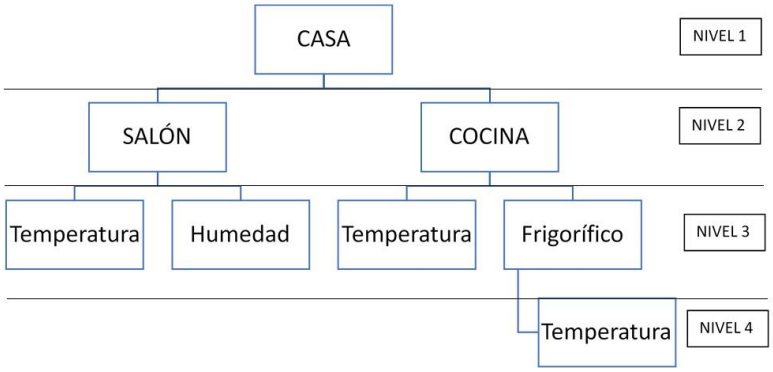


Fuente: Autor

Una cosa muy interesante es la posibilidad de jerarquizar los topic (figura 2), separándolos con una barra (‘/’), lo que permite crear una estructura de topic escalable, permitiendo añadir o eliminar elementos de la red de comunicación sin afectar a los otros elementos. Como ejemplo de ello, se puede ver en la figura 3 una estructura correspondiente a una casa que se miden distintos parámetros del salón y cocina, de la que resultan los siguientes topics:

- CASA/SALÓN/Temperatura
- CASA/SALÓN/Humedad
- CASA/COCINA/Temperatura
- CASA/COCINA/Frigorífico/Temperatura

Figura 3. Ejemplo de estructuras de nivel o topics



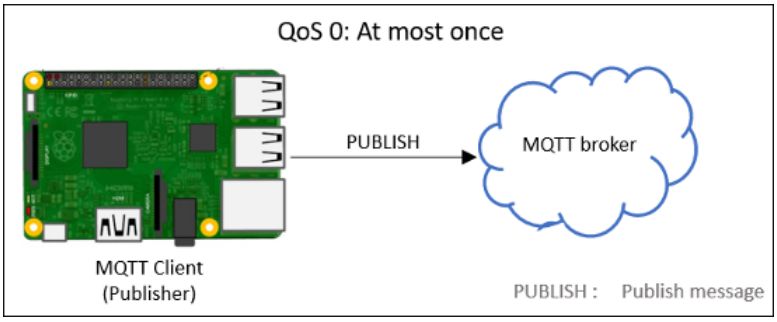
Fuente: Autor

A la hora de suscribirse existen dos comodines para sustituir un nivel de jerarquía o varios, según se desee. Estos comodines solo pueden ser usados por los suscriptores y no por los clientes que publican mensajes en un topic, el cual debe ser conciso.

Nivel de QoS para publicar

El nivel QoS 0 (figura 4), el editor envía el mensaje al intermediario MQTT como máximo una vez, sin embargo, no es suficiente para que el intermediario reconozca la recepción del mensaje.

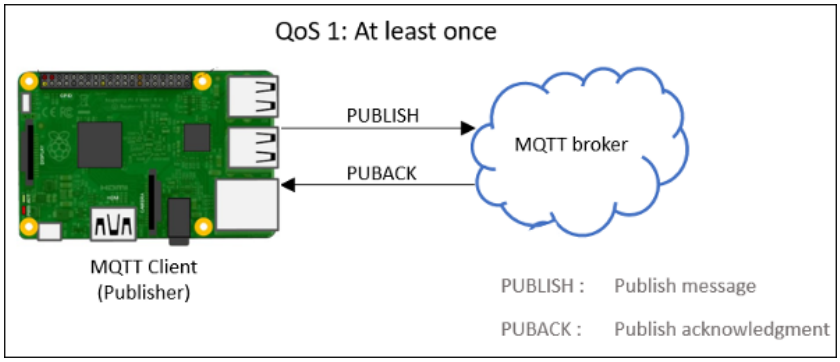
Figura 4. Nivel de QoS 0 para publicar



Fuente: Autor

En el nivel QoS 1 (figura 5), el publicador envía el mensaje al intermediario MQTT al menos una vez. El editor almacena el mensaje hasta que recibe una confirmación del intermediario. Si no se recibe ninguna confirmación después de 10 segundos, el publicador vuelve a enviar el mensaje. En este nivel, el mismo mensaje podría entregarse al intermediario más de una vez.

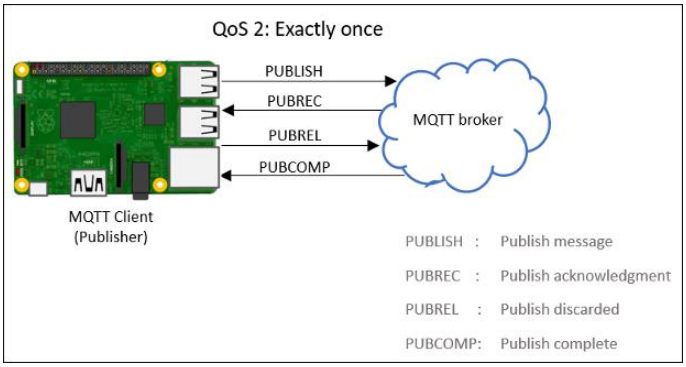
Figura 5. Nivel de QoS 1 para publicar



Fuente: Autor

En el nivel QoS 2 (figura 6), el publicador envía el mensaje al intermediario MQTT exactamente una vez. El editor almacena el mensaje hasta que obtiene una confirmación del intermediario. Una vez recibida la confirmación, el editor y el intermediario descartan los mensajes almacenados. QoS2 utiliza confirmaciones adicionales para asegurarse de que no se entrega ningún mensaje duplicado al intermediario.

Figura 6. Nivel de QoS 2 para publicar

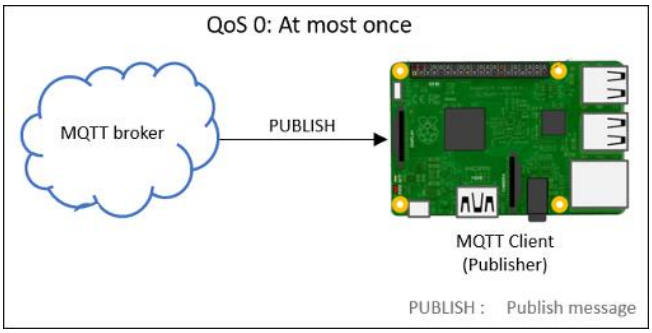


Fuente: Autor

Nivel de QoS para suscribirse

Para el nivel QoS 0 (figura 7), el intermediario MQTT envía el mensaje al cliente como máximo una vez, lo que hace que el cliente no reconozca la recepción del mensaje.

Figura 7. Nivel de QoS 0 para suscribirse

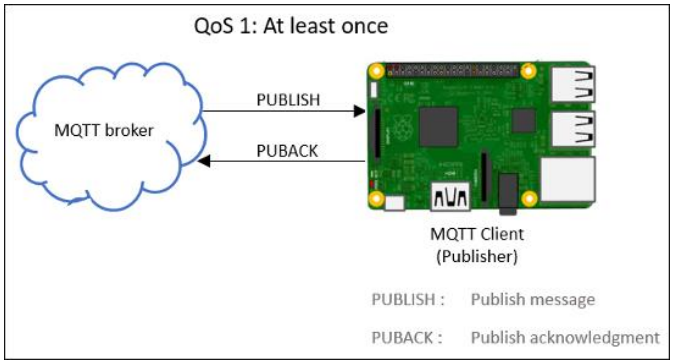


Fuente: Autor

En el nivel QoS 1 (figura 8), el intermediario MQTT envía el mensaje al cliente al menos una vez. El intermediario MQTT almacena el mensaje hasta que obtiene una confirmación del cliente. Si no

se recibe ninguna confirmación después de 10 segundos, el intermediario vuelve a enviar el mensaje. En este nivel, el mismo mensaje podría entregarse más de una vez.

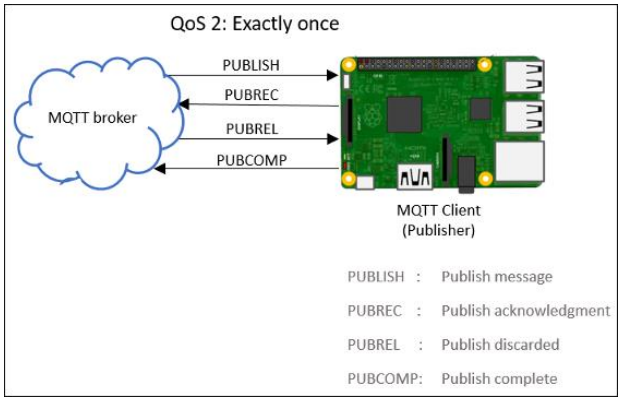
Figura 8. Nivel de QoS 1 para suscribirse



Fuente: Autor

Dentro del nivel QoS 2 (figura 9), el intermediario MQTT envía el mensaje al cliente exactamente una vez. El intermediario MQTT almacena el mensaje hasta que obtiene una confirmación del cliente. Una vez que se recibe el acuse de recibo, el intermediario y el suscriptor descartan los mensajes almacenados. QoS2 utiliza confirmaciones adicionales para asegurarse de que no se entrega ningún mensaje duplicado.

Figura 9. Nivel de QoS 2 para suscribirse



Fuente: Autor

Problema o necesidad

El internet de las cosas, es una red de elementos físicos con identificadores únicos y la capacidad de transferir datos a la red sin requerir de la intervención humana. Esta red converge de objetos y personas conectados para enviar y recibir datos, requiere una participación importante de las tecnologías web que permitan a través de una conexión remota acceder a servicios y aplicaciones para monitorizar y controlar los dispositivos conectados al IoT. De esta manera, en la capa de aplicación de la arquitectura tecnológica del IoT existen protocolos y tecnologías que son necesarios para manejar la comunicación entre objetos. Por lo que se requiere un estudio de estos protocolos, que con parámetros establecidos de acuerdo a un cierto tipo de aplicación IoT, permitan escoger la mejor tecnología para su desarrollo.

Con estos antecedentes, el principal problema de la heterogeneidad de datos en la interconexión de dispositivos IoT obtenidos a través de sensores, es uno de los aspectos que se mejoran mediante descripciones semánticas y modelos de conocimiento. Es a partir de este conocimiento que existen organizaciones dedicadas a aportar tecnologías ontológicas para que sea unificadas y utilizadas en el desarrollo de aplicaciones IoT

Metodología

Evaluación preliminar

Para el desarrollo de este trabajo se ha optado por una investigación cualitativa, ya que, al realizar un estudio comparativo de las diferentes tecnologías para el envío de datos en el Internet de las cosas, se requiere de un análisis de las características que permitan mejorar la comunicación entre objetos, es decir hablamos de un análisis de texto y otros aspectos que intervienen en este proceso. De igual manera, para el planteamiento del uso de aspectos de seguridad mediante el protocolo MQTT en el aplicativo de internet de las cosas, se aplica procedimientos basados en una investigación cuantitativa e interpretación sistemática.

La revisión del estado del arte es de tipo bibliográfica y descriptiva, que emerge en la exploración exhaustiva de la información asociada con las estrategias fundamentales para la seguridad de los sistemas domóticos, empleando la revisión sistemática de la literatura para examinar los estándares asociados en el de desarrollo de los sistemas autónomos para hogares inteligentes. Para lo cual, se emplea el método analítico que inspecciona los objetivos de Gobierno y las decisiones de TI, que

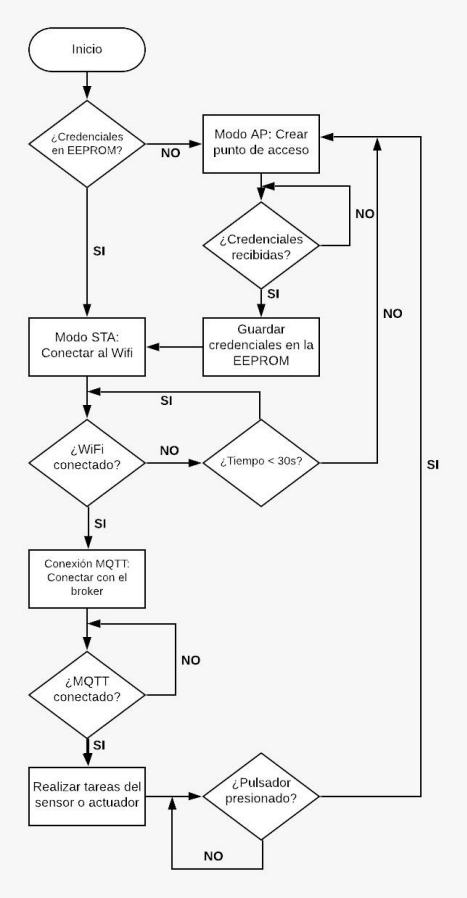
fundamentan las buenas prácticas inmersas en la seguridad de los sistemas en cuestión, de la integridad de los datos, la fiabilidad de los procedimientos y la confiabilidad de los servicios.

Resultados

Es importante señalar que no se puede determinar cuál es el mejor protocolo para el envío de mensajes, ya que el ambiente de IoT es tan diverso que dependiendo al campo en que se vaya a utilizar el protocolo, resultará beneficioso en unos casos y en otros no.

Dentro del trabajo de investigación se plantea la siguiente propuesta de IoT aplicado MQTT (figura 10).

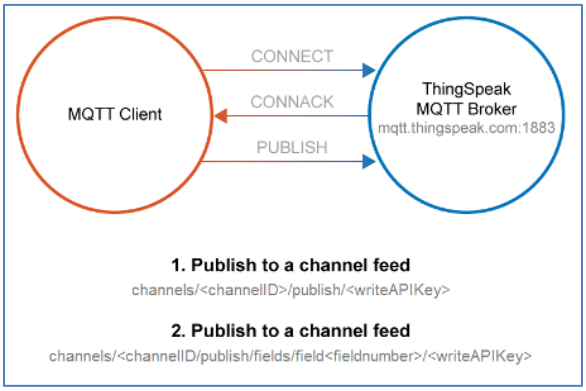
Figura 10. Diagrama de flujo de la propuesta IoT con MQTT



Fuente: Autor

Dentro del proceso de aplicación IoT, primero se debe describir la estructura de configuración de la clave API (figura 11) de escritura para publicar, en donde, el intermediario reconoce una solicitud CONNECT correcta con CONNACK.

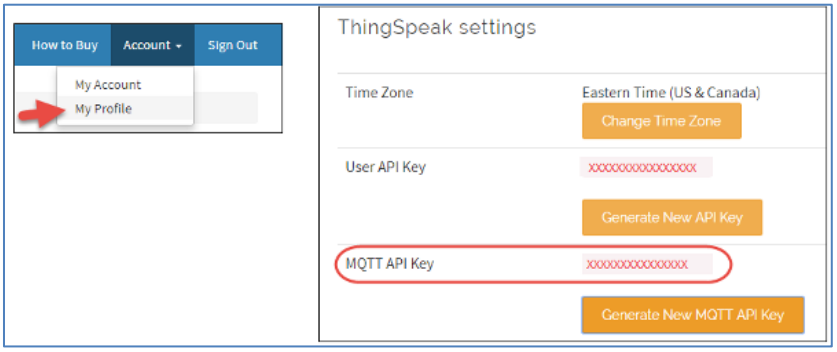
Figura 11. Publicación MQTT



Fuente: Mathwoks, 2019

El siguiente paso es describir la estructura del tema, suscribiéndose a un canal público o privado, proporcionando un nombre de usuario y su clave de API MQTT como contraseña cuando se conecte.

Figura 12. Suscripción MQTT



Fuente: Mathwoks, 2019

Finalmente, si la conexión se realiza correctamente, el intermediario MQTT de ThingSpeak responde con un CONNACK, una confirmación de conexión. El intermediario MQTT responde a una solicitud de suscripción correcta con un mensaje SUBACK y retransmite al cliente los datos nuevos publicados en el canal o campo suscrito. ThingSpeak tiene un intermediario MQTT en la

dirección URL mqtt.thingspeak.com, donde podemos configurar al cliente MQTT para comunicarse con el intermediario MQTT de ThingSpeak en función de una de las siguientes opciones (Tabla 2):

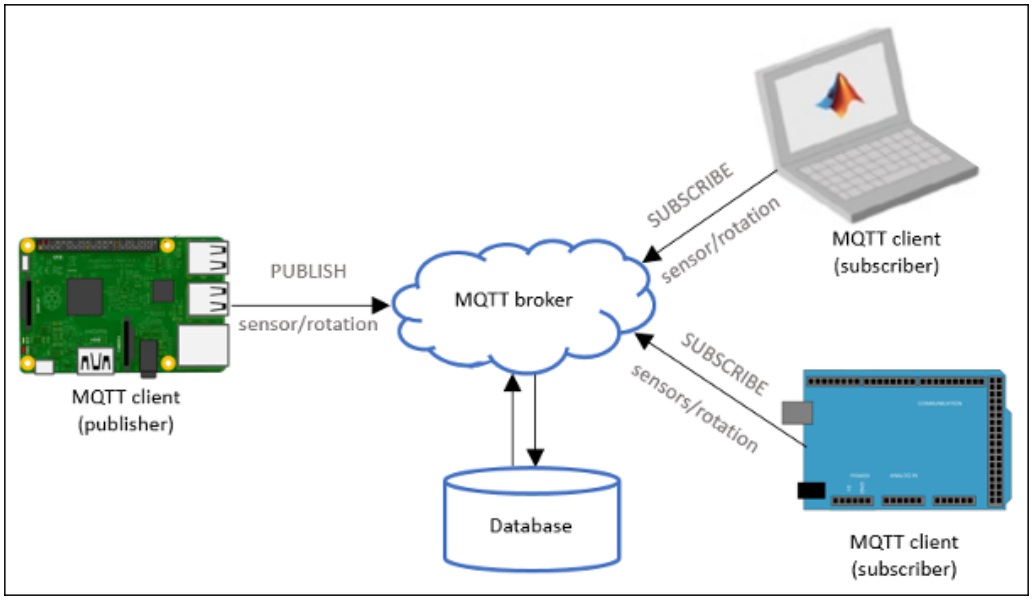
Tabla 2. Configuración del cliente MQTT

Port	Connection Type	Encryption
1883	TCP	None
8883	TCP	TLS/SSL
80	WebSocket	None
443	WebSocket	TLS/SSL

A. Integración de ThingSpeak mediante bloques MQTT, Rasberry Pi y Simulink

Para la integración macro de IoT (figura 13), usamos ThingSpeak como intermediario entre MQTT y Raspberry es el cliente MQTT (editor y suscriptor). Simulink Support Package para Raspberry Pi proporciona una manera fácil de crear algoritmos que utilizan periféricos Raspberry Pi mediante el uso de bloques que se pueden agregar a su modelo de raspberry. Los bloques se utilizan para configurar los sensores y actuadores asociados, así como para leer y escribir datos en ellos.

Figura 13. Configuración de un sistema domótico mediante el protocolo MQTT

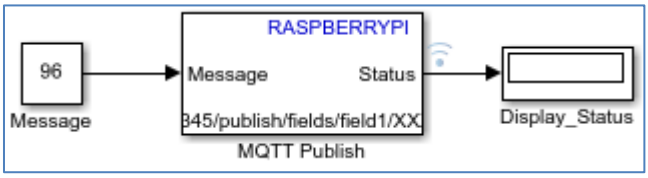


Fuente: Autor

Para la simulación del sistema, nos apoyamos del software Matlab 2018a, para lo cual primero conectamos el cable micro USB al puerto micro USB del hardware Raspberry Pi, y el otro extremo

del cable al ordenador; se debe esperar a que el LED de alimentación de Raspberry Pi permanezca sólido y finalmente conectar el puerto Ethernet de Raspberry Pi a una LAN con acceso a Internet. El siguiente paso (figura 14) es crear el modelo de mensajes MQTT Publish.

Figura 14. Publicación de mensaje a bróker MQTT



Fuente: Autor

El bloque MQTT Publish acepta un mensaje de tipo de datos uint8 que se publicará en el bróker (figura 15).

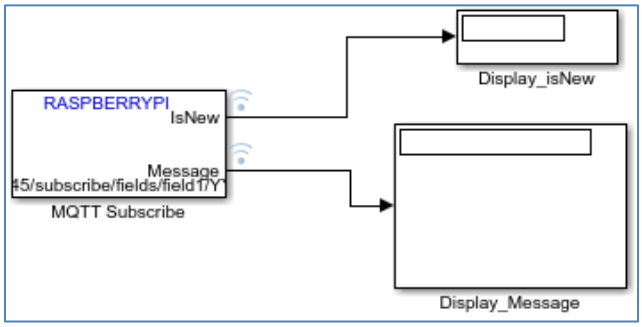
Figura 15. Parámetros del bloque MQTT Publish

Parameter	Value	Description
Topic	channels/12345/publish/fields/field1/XXXXXXXXXX	The topic to which Raspberry Pi publishes the message.
		The topic must follow the format:
		channels/<channelID>/publish/fields/field<fieldNumber>/<writeAPIKey>
		In this example,
		* channelID is specified as 12345.
		* fieldNumber is specified as 1. You can specify any number from 1 to 8.
		* writeAPIKey is specified as XXXXXXXXXX.
QoS	0	The ThingSpeak MQTT broker supports only QoS 0.
Retain Msg	off	The ThingSpeak MQTT broker does not support retain message flag.

Fuente: Autor

Posteriormente, se crea el modelo MQTT suscribe como se muestra en la Figura 16 y 17.

Figura 16. Suscribirse al mensaje de ThingSpeak MQTT Broker



Fuente: Autor

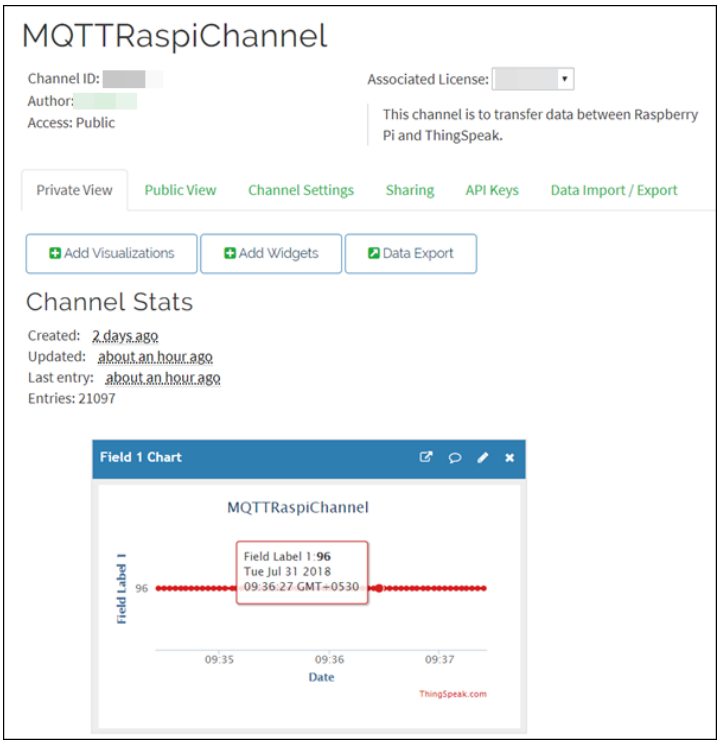
Figura 17. Parámetros del bloque MQTT Subscribe

Parameter	Value	Description
Topic	channels/12345/subscribe/fields/field1/YYYYYYYYYY	The topic to which Raspberry Pi subscribes.
		The topic must follow the format:
		channels/<channelID>/subscribe/fields/field<fieldNumber>/<readAPIKey>
		In this example,
		* channelID is specified as 12345.
		* fieldNumber is specified as 1. You can specify any number from 1 to 8.
		* readAPIKey is specified as YYYYYYYYYY.
QoS	0	The ThingSpeak MQTT broker supports only QoS 0.
Message length (N)	1	The length of the message to be received.
Sample time	1	Raspberry Pi(TM) receives the message from the ThingSpeak MQTT broker every one second.

Fuente: Autor

Una vez construido el modelo, se procede a compilar, iniciar e implementar el modelo en Raspberry Pi, publicando el mensaje en el campo 1 del broker MQTT de ThingSpeak (figura 18)

Figura 18. Visualización del mensaje o estatus del bróker MQTT



Fuente: Autor

Discusión

La seguridad de los sistemas domóticos constituye un proceso de establecer estrategias, políticas, técnicas, normativas o procedimientos que direccionen el desarrollo de sistemas sólidos que garanticen en mayor medida el correcto funcionamiento de los servicios y la optimización de sus recursos.

Aunque todavía estamos lejos de la extensiva implantación de domótica en espacios domésticos en nuestro país, es habitual proyectar las nuevas tecnologías en el hogar hacia la gestión del confort, el uso óptimo de la energía, la integración de las redes de datos y las comunicaciones como lo manifiesta Romero Morales, Vázquez Serrano y De Castro Lozano (2006).

Es por ello, que la adopción de un plan de gobierno de TI establece una estrategia de integración que agrega valor significativo en minimizar los riesgos y proporcionar servicios de TI eficientes, lo que constituye un eje primordial para que los desarrolladores proyecten cada uno de sus procesos en lineamientos que fomentan el mejoramiento de la productividad y la calidad de los servicios

Conclusiones

Los sistemas domóticos en el hogar se encuentran centrados en la automatización y el control de aplicaciones y múltiples dispositivos, por lo cual la seguridad es una característica esencial para la protección e integridad del usuario y la vivienda.

A través del proceso investigativo se identifica ciertas dificultades en la implementación y desarrollo de los sistemas domóticos tales como acceso no autorizado, interfaces y configuraciones complejas, confiabilidad propensa e interoperabilidad de los dispositivos.

Son varias las situaciones por la cual un sistema posee niveles bajos de seguridad, siendo necesario cubrir esta deficiencia a través de procedimientos, gestiones, estándares o normativas que determinan procesos pertinentes para la efectividad e integridad de los recursos, para lo cual es necesario analizar las normas o buenas prácticas con mayor asociación y adaptabilidad a las actividades de gestión involucradas.

Uno de los protocolos con mayor adopción en el campo de la domótica es MQTT que permite una comunicación óptima de mensajería asíncrona con seguridad integrada dada a la flexibilidad y simplicidad que permite la integración de los dispositivos dentro de la red doméstica en los hogares inteligentes.

Referencias

1. C. Romero Morales, J. Vázquez Serrano y C. De Castro Lozano, Domótica e inmótica. Viviendas y Edificios Inteligentes, Segunda ed., RA-MA S.A., 2006, p. 416.
2. M. Wulff-Pérez , A. Martín-Rodriguez, M. J. Gálvez-Ruiz y J. de Vicente, «The effect of polymer surfactant on the rheological properties of nanoemulsions.,» Colloid and Polymer Science, vol. 291, p. 709–716, 2013 .
3. V. Zamora Mora, P. I. Soares, C. Echeverria, R. Hernández y C. Mijangos, «Composite chitosan/Agarose ferrogels for potential applications in magnetic hyperethermia,» Gels., vol. 1, pp. 69-80, 2015.
4. S. Bhat, A. Tripathi y A. Kumar, «Supermacroprous chitosan-agarose-gelatin cryogels. in vitro characterization and in vivo assesment for cartilage tissue engineering.,» Journal of the Royal Society Interface, pp. 1-15, 2010.
5. G. A. Ruiz Estrada, «Desarrollo de un Sistema de liberación de fármacos basado en nanopartículas magnéticas recubiertas con Polietilénglicol para el tratamiento de diferentes enfermedades.,» Universidad Autónoma de Madrid. Departamento de Física Aplicada., Madrid, 2004.
6. J. A. Cortés, J. E. Puig, J. A. Morales y E. Mendizábal, «Hidrogeles nanoestructurados termosensibles sintetizados mediante polimerización en microemulsión inversa.,» Revista Mexicana de Ingeniería Química., vol. 10, nº 3, pp. 513-520, 2011.
7. J. Song , S. u. King, S. Yoon , D. Cho y Y. Jeong, «Enhanced spinnability of narbon nanotube fibers by surfactant addition,» Fiberes and Polymers, vol. 15, nº 4, pp. 762-766, 2014.
8. P. Ilg, «Stimuli-responsive hydrogels cross-linked by magnetic nanoparticles.,» Soft Matter, vol. 9, pp. 3465-3468, 2013.
9. G. Bossis, J. A. Marins, P. Kuzhir, O. Volkova y A. Zubarev, «Functionalized microfibers for field-responsive materials and biological applications.,» Journal of Intelligent Material Systems and Structures, pp. 1-9, 2015.
10. Y.-S. Lin, K.-S. Huang, C.-H. Yang, C.-Y. Wang, Y.-S. Yang, H.-C. Hsu, Y.-J. Liao y C.-W. Tsai, «Microfluidic synthesis of microfibers for magnetic-responsive controlled drug release and cell culture.,» PLoS ONE, vol. 7, nº 3, pp. 1-8, 2012.

11. P. Tartaj, M. P. Morales, T. González-Carreño, S. Veintemillas-Verdaguer y C. J. Serna, «Advances in magnetic nanoparticles for biotechnology applications.,» Journal of Magnetism and Magnetic Materials, vol. 290, pp. 28-34, 2005.
12. L. García-Cerda, O. Rodríguez-Fernández, R. Betancourt-Galindo, R. Saldívar-Guerrero y M. Torres-Torres, «Síntesis y propiedades de ferrofluidos de magnetita,» Superficies y Vacío., vol. 16, nº 1, pp. 28-31, 2003.
13. A. Dias, A. Hussain, A. Marcos y A. Roque, «A biotechnological perspective on the application of iron oxide magnetic colloids modified with polysaccharides.,» Biotechnology Advances 29 , vol. 29, p. 142–155, 2011.
14. D. Y. Lewitus, J. R. Branch, K. L. Smith, G. Callegari, J. Kohn y A. V. Neimark, «Biohybrid carbon nanotube/agarose fibers for neural tissue engineering.,» Advanced Functional Materials, vol. 21, pp. 2624-2632, 2011.
15. R. F. Estrada Guerrero, D. Lemus Torres, D. Mendoza Anaya y V. Rodriguez Lugo, «Hidrogeles poliméricos potencialmente aplicables en Agricultura.,» Revista Iberoamericana de Polímeros, vol. 12, nº 2, pp. 76-87, 2010.
16. S. Aldana, F. Vereda, R. Hidalgo-Alvarez y J. de Vicente, «Facile synthesis of magnetic agarose microfibers by directed selfassembly,» Polymer, vol. 93, pp. 61-64, 2016.
17. C. R. Cabello, «https://www.sage.com/es-es/blog/infografia-factura-tradicional-vs-factura-electronica-estas-son-las-principales-diferencias/,» 12 06 2018. [En línea]. Available: www.gase.com.
18. A. Barreix and R. Zambrano, "Centro Internacional de Administraciones Tributaria," 21 marzo 2018. [Online]. Available: https://www.ciat.org/la-factura-electronica-en-america-latina/#comments.
19. L. D. R. T. SRI, «file:///C:/Users/Dario/Downloads/LEY%20DE%20R%C3%89GIMEN%20TRIBUTARIO%20INTERNO%20%C3%BAltima%20actualizaci%C3%B3n%208%20de%20septiembre%20de%202017.pdf,» 20 septiembre 2017. [En línea]. Available: www.arancelecuador.com.
20. 2.-F.-2. Registro Oficial 448, «Registro Oficial 448, 28-Febrero-2015,» 28 febrero 2015. [En línea].

21. W. Dent, «CONSUMER-BASE SYSTEM AND METHOD FORMANAGING AND PAYING ELECTRONIC BILLING STATEMENTS». United States Patent Patente 6,128,603, 9 septiembre 1997.
22. Yi-Hung, Q. Leng and S. Han, "RT-WIFI:REAL-TIME High-Speed Communication Protocol for Wireless Cyber-Physical Control Applications," in 34° Simposio de sistemas en tiempo real de IEEE, Vancouver,BC, Canadá, 2014.
23. GRUPO SERES, «ec.grupseres.com,» 29 10 2019. [En línea]. Available: https://ec.groupseres.com/facturaelectronica/normativa.
24. M. A. Flórez de la Colina, «Hacia una definición de la domótica,» Informes de la Construcción, 2004.
25. L. F. Herrera Quintero, «Viviendas inteligentes (Domótica),» Revista Ingeniería e Investigación, vol. 25, pp. 47-53, 2005.
26. M. Barrera Durango, N. Londoño Ospina, J. Carvajal y A. Fonseca, «Análisis y diseño de un prototipo de sistema domótico de bajo costo,» Revista Facultad de Ingeniería Universidad de Antioquia, pp. 117-128, 2012.
27. W. Edwards y R. Grinter, «At Home with Ubiquitous Computing: Seven Challenges,» de International Conference Atlanta Georgia, USA, 2001.
28. G. B. Asencio, J. Maestre, J. M. Escaño, C. Martín Macareno, M. Molina y E. Camacho, «Interoperabilidad en Sistemas Domóticos mediante Pasarela Infrarrojos-ZigBee,» Revista Iberoamericana de Automática e Informática Industrial RIAI, vol. 8, nº 4, pp. 397-404, 2011.
29. A. Guedez, «GB Advisors,» 2018. [En línea]. Available: https://www.gb-advisors.com/es/normas-y-estandares-internacionales/.
30. IECOR, «Estándares Internacionales de Domótica,» 2007-2016. [En línea]. Available: https://www.iecor.com/estandares-internacionales-de-domotica/.
31. W. Harke, Domótica para Viviendas y Edificios, Barcelona: Marcombo, 2010.
32. M. Yuan, «IBM,» 04 Octubre 2017. [En línea]. Available: https://www.ibm.com/developerworks/ssa/library/iot-mqtt-why-good-for-iot/index.html.
33. O. Sadio, I. Ngom y C. Lishou, «Lightweight Security Scheme for MQTT/MQTT-SN Protocol,» de Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), 2019.

34. D. I. Dikii, «Denial of service attack analysis by MQTT protocol,» Scientific and Technical Journal of Information Technologies, Mechanics and Optics, vol. 20, nº 2, p. 223–232 , 2020.
35. T. Vadluri, «Implementation of Home Automation System using MQTT Protocol and ESP32,» International Journal of Engineering and Advanced Technology (IJEAT), vol. 8, 2018.
36. C. Espinoza Aguirre y F. Iñiguez Matute, «Implementación de Gobierno de TI,» Revista Bitácora Académica - USFQ, vol. 2, nº 1, 2018.
37. S. Junestrand, X. Passaret y D. Vázquez, Domótica y hogar digital, España: Paraninfo, 2004.
38. S. Cadena-Vela y R. Enríquez-Reyes, «Diseño e implementación de un centro de datos en la Universidad Central del Ecuador,» de Congreso Ecuatoriano de Tecnologías de Información y Comunicación, 2017.
39. E. R. Gaseta, A. C. Motta y J. D. Boca Piccolini, Fundamentos de Gobierno de TI, Colombia: Red Nacional de Tecnología Avanzada, 2014.
40. F. Mateos Martín, M. García Prado, R. Mayo Bayón, R. Poo Argüelles y V. González Suárez, «Software tools for PLC Programming and Internet HMI in Domotics,» de IFAC Proceedings Volumes, España, 2002.