ANTEPROYECTO DEL TRABAJO DE FIN DE GRADO

INFORMACIÓN GENERAL					
Alumno/a	Romero Luque, Diego Jesús				
Titulación:	Grado ingeniería informática				
Tutor/es:	Davide Ferraris				
Título	Autorización basada en la confianza para el protocolo MQTT				
Subtítulo *(solo si en grupo)*					
Título en inglés	Trust based authorization for the MQTT protocol				
Subtítulo en inglés *(solo si en grupo)*					
Trabajo en grupo:	**Sí**		**No**	X	
Otros integrantes del grupo:					

INTRODUCCIÓN

Contextualización del problema a resolver. Describir claramente de dónde surge la necesidad de este TFG y el dominio de aplicación. En caso de que el TFG se base en trabajos previos, debe aclararse cuáles son las aportaciones del TFG.

El Internet de las Cosas (IoT) es un paradigma tecnológico que permite la interconexión de dispositivos a través de redes. Estos dispositivos pueden obtener, intercambiar y procesar datos para automatizar procesos y mejorar la eficiencia en numerosos sectores como la industria, la agricultura o el hogar [1].

En un entorno IoT, los dispositivos deben comunicarse para compartir información y coordinar acciones. Estas comunicaciones pueden implicar sensores, actuadores o servidores. Debido al carácter distribuido y heterogéneo de las redes IoT, estas comunicaciones representan un reto técnico y de seguridad[2].

Uno de los protocolos más usados es MQTT (Message Queuing Telemetry Transport). Es un protocolo ligero de mensajería, está diseñado para conexiones con dispositivos con recursos limitados y en redes inestables. Su arquitectura se basa en el modelo publicador/suscriptor [3]. Todo esto lo que lo convierte en una opción ideal para aplicaciones IoT.

En este tipo de redes, donde los dispositivos actuan de forma autónoma, el concepto de confianza se vuelve esencial. La confianza permite establecer criterios sobre el comportamiento esperado de los dispositivos, evaluando su fiabilidad. Incorporar un modelo de confianza permite mejorar los mecanismos de seguridad y control de acceso, al identificar dispositivos potencialmente maliciosos o comprometidos [4].

Este trabajo tiene como objetivo implementar un sistema de control de acceso basado en la confianza para IoT [5] usando el protocolo MQTT como base. La solución incluirá mecanismos de autenticación y autorización de dispositivos. Además, se implementará una interfaz web que permita a los usuarios visualizar y gestionar los parámetros relevantes del sistema.

OBJETIVOS

Descripción detallada de en qué consistirá el TFG. En caso de que el objeto principal del TFG sea el desarrollo de software, además de los objetivos generales deben describirse sus funcionalidades a alto nivel.

El TFG tiene varios objetivos, todos relacionados con un sistema de control de acceso para IoT basando en la confianza y el protocolo MQTT:

- Creación de un modelo de confianza apropiado para MQTT.
- Implementar un sistema de control de acceso como una extensión del broker HiveMQ, basado en el modelo de confianza descrito anteriormente.
- Desarrollo de una interfaz web donde se podrán visualizar y editar ciertos atributos del modelo.

ENTREGABLES

Listado de resultados que generará el TFG (aplicaciones, estudios, manuales, etc.)

Extension para HiveMQ

Web de control

Memoria

Manuales de uso

MÉTODOS Y FASES DE TRABAJO

METODOLOGÍA:

Descripción de la metodología empleada en el desarrollo del TFG. Especificar cómo se va a desarrollar. Concretar si se trata de alguna metodología existente y, en caso contrario, describir y justificar adecuadamente los métodos que se aplicarán.

Para el desarrollo del trabajo se usará la metodología scrum, con ayuda de la web trello.com. El proyecto se divide en diferentes tareas, las cuales organizan en las columnas del tablero según el estado y la prioridad de estas. Los sprints tendrán una duración de 2 semanas y en ellos se realizarán las tareas que se decidan al comienzo de este sprint.

FASES DE TRABAJO:

Enumeración y breve descripción de las fases de trabajo en las que consistirá el TFG.

- **Sprint 1: Pasos preliminares**
  - Estado del arte
  - Definición de requisitos
  - Definición de casos de uso
- **Sprint 2: Diseño del sistema**
  - Modelo de confianza
  - Modelo de control de acceso
  - Definir protocolo de control de atributos
  - Creación de diagramas

- **Sprint 3: Implementar sistema base**
  - Implementar autenticación de dispositivos
  - Implementar cálculo de atributos
  - Implementar persistencia de datos

- **Sprint 4: Desarrolo todas las funciones del sistema**
  - Implementar modelo de confianza
  - Implementar control de acceso
  - Implementar capa de control

- **Sprint 5: Implementación de clientes**
  - Desarrollo web de control
  - Desarrollar cliente

- **Sprint 6: Análisis y documentación**
  - Análisis de rendimiento
  - Manual de uso
  - Elaborar memoria

TEMPORIZACIÓN:

La siguiente tabla deberá contener una fila por cada una de las fases enumeradas en la sección anterior. En caso de tratarse de un trabajo en grupo, se añadirá una columna HORAS por cada miembro del equipo. Debe especificarse claramente el número de horas dedicado por cada alumno/a y la suma de horas individual deberá ser también de 296.

FASE	HORAS
Estado del arte	**10**
Modelo de confianza	**10**
Modelo de control de acceso	**10**
Definir protocolo de control de atributos	**10**
Definición de requisitos	**15**
Definición de casos de uso	**15**
Creación de diagramas	**20**
Implementar autenticación de dispositivos	**10**
Implementar cálculo de atributos	**30**
Implementar persistencia de datos	**10**
Implementar modelo de confianza	**30**
Implementar control de acceso	**20**
Implementar protocolo de control de atributos	**15**
Desarrollo web de control	**35**
Desarrollar cliente	**15**
Análisis de rendimiento	**10**
Manual de uso	**6**
Elaborar memoria	**25**
	296

ENTORNO TECNOLÓGICO
TECNOLOGÍAS EMPLEADAS:
Enumeración de las tecnologías utilizadas (lenguajes de programación, frameworks, sistemas gestores de bases de datos, etc.) en el desarrollo del TFG.
Java
MQTT
Base de datos SQL
Svelte
TypeScript
RECURSOS SOFTWARE Y HARDWARE:
Listado de dispositivos (placas de desarrollo, microcontroladores, procesadores, sensores, robots, etc.) o software (IDE, editores, etc.) empleados en el desarrollo del TFG.
Intellij Idea
HiveMq
Maven
Docker
trello

REFERENCIAS
Listado de referencias (libros, páginas web, etc.)
1. Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The internet society (ISOC)*, *80*(15), 1-53
2. Čolaković, A., & Hadžialić, M. (2018). Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. Computer networks, 144, 17-39.
3. Soni, D., & Makwana, A. (2017, April). A survey on mqtt: a protocol of internet of things (iot). In *International conference on telecommunication, power analysis and computing techniques (ICTPACT-2017)* (Vol. 20, pp. 173-177)
4. Ferraris, D., Fernandez-Gago, C., Roman, R., & Lopez, J. (2024). A survey on IoT trust model frameworks. *The Journal of Supercomputing*, *80*(6), 8259-8296
5. Bernal Bernabe, J., Hernandez Ramos, J. L., & Skarmeta Gomez, A. F. (2016). TACIoT: multidimensional trust-aware access control system for the Internet of Things. *Soft Computing*, *20*, 1763-1779

Málaga, _____ de _____ de _____

Firma tutor/tutora: Firma cotutor/a: Firma tutor/a coordinador/a: