ANTEPROYECTO DEL TRABAJO DE FIN DE GRADO

INFORMACIÓN GENERAL					
Alumno/a	Diego González Rodríguez				
Titulación:	Grado en Ingeniería Informática				
Tutor/es:	María del Carmen Fernández Gago Davide Ferraris				
Título	Gestor de confianza para dispositivos IoT, mediante el protocolo MQTT				
Subtítulo *(solo si en grupo)*					
Título en inglés	Trusted manager for IoT devices, using 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.

La necesidad de incrementar la seguridad en entornos de IoT (Internet de las Cosas) surge debido al alto crecimiento de la adopción de este tipo de dispositivos interconectados como, por ejemplo: electrodomésticos, cámaras de seguridad, termostatos… en hogares inteligentes, sector de la industria o entornos similares, recopilando y almacenando datos de forma constante.

El objetivo principal de este trabajo es desarrollar modelos y métricas de confianza específicamente diseñados para entornos de IoT, destinados a mejorar la seguridad. Algunas de las contribuciones más destacables son:

1. **Desarrollo de Modelos de Confianza:** Se crearán modelos de confianza que utilizan enfoques como el cálculo de reputación y el intercambio de políticas de seguridad. Estos modelos están diseñados para evaluar la confiabilidad de los dispositivos y entidades dentro de un entorno de IoT que además puede ser dinámico, determinando así si es posible o no establecer una comunicación entre dichos dispositivos o es más conveniente rehusarla y actuando en consecuencia. Además, estos modelos podrán reutilizarse para facilitar la definición de situaciones similares, ahorrando trabajo de esta forma y será posible que interactúen entre sí.
2. **Métricas de Confianza:** Se definirán métricas específicas para evaluar la confianza en un entorno de IoT. Estas métricas podrían abordar aspectos como la integridad de los datos, la autenticidad de los dispositivos, o la capacidad de respuesta a amenazas de seguridad.
3. **Simulación de Entornos:** Dado que la implementación directa en entornos de producción es algo muy arriesgado, se utilizarán entornos simulados para evaluar los modelos de confianza, proporcionando así un entorno controlado para probar la eficacia y la viabilidad de estos.

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.

1. Desarrollar Modelos de Confianza: implementar modelos de confianza basados en el cálculo de reputación y el intercambio de políticas de seguridad. Estos modelos evaluarán la confiabilidad de dispositivos y entidades en entornos dinámicos de IoT.

2. Definir Métricas de Confianza: crear métricas específicas para cuantificar la confianza en un entorno de IoT. Estas métricas abordarán aspectos clave como la integridad de los datos, autenticidad de los dispositivos y capacidad de respuesta a amenazas de seguridad.

3. Desarrollar Software de Evaluación de Confianza: haciendo uso de Java como lenguaje de programación y el protocolo MQTT para la comunicación, desarrollando un software que evalúe la confianza entre dispositivos en entornos dinámicos de IoT. Este software será capaz de conectarse a entornos simulados para realizar pruebas controladas.

4. Integración con Entornos Simulados: implementar la integración del software con entornos simulados, utilizando placas Arduino/Raspberry o softwares de simulación. Estos ayudarán a entender y tratar las complejidades del mundo real, permitiendo pruebas realistas y controladas.

5. Validar Eficacia y Viabilidad: realizar pruebas exhaustivas para validar la eficacia y viabilidad de los modelos y métricas desarrollados antes de considerar la implementación en entornos de producción.

6. Generar Conclusiones y Datos: extraer conclusiones significativas y datos relevantes a partir de las pruebas realizadas en los entornos simulados. Estos resultados servirán como base para futuras decisiones y posibles implementaciones en entornos reales de IoT.

7. Documentar el Proceso: elaborar una documentación detallada que describa el proceso de desarrollo, las decisiones tomadas, los resultados obtenidos y las lecciones aprendidas durante el transcurso del TFG.

ENTREGABLES

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

Documentación:

- Un informe detallado que abarque el diseño y la implementación de los modelos de confianza, así como la definición de las métricas propuestas.
- Documentación sobre el uso de Java y el protocolo MQTT en el desarrollo del código.

Código Fuente:

- El código fuente del proyecto desarrollado en Java, que incluye la implementación de los modelos de confianza, las métricas y la lógica de integración con el protocolo MQTT.

Simulaciones y Resultados:

- Información detallada sobre las simulaciones realizadas, ya sea con placas Arduino/Raspberry Pi o software de simulación, y los resultados obtenidos, pudiéndose incluir gráficos, estadísticas y conclusiones extraídas de las pruebas.

Presentación Oral:

- Una presentación que resuma los objetivos, métodos y resultados del proyecto de cara a la defensa del TFG.

Conclusiones y Trabajo Futuro:

- Un apartado que resuma las conclusiones extraídas del proyecto y posibles áreas de mejora o expansión en el futuro.

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.

La metodología que se va a emplear se basará en una combinación de metodologías ágiles y buenas prácticas de desarrollo de software, esto es debido a la naturaleza de los sistemas IoT, que a menudo involucran dificultades y desafíos únicos. Siguiendo un enfoque iterativo es posible abordar estos retos pudiendo ajustar el enfoque a medida que se entienden y resuelvan los problemas encontrados.

Además, se contará con una evaluación continua y retroalimentación por parte de los tutores y profesores, facilitando así la mejora constante y la adaptación a medida que se obtienen nuevos conocimientos. Dado que el TFG se centra en el desarrollo de modelos de confianza, este enfoque permite una mayor flexibilidad para reflejar la dinámica cambiante de los entornos IoT y las amenazas asociadas.

A continuación, se detalla la metodología propuesta:

1. **Definición de requisitos:**
   - Identificación y definición clara de los requisitos del sistema, enfocándose principalmente en la seguridad en entornos IoT y los objetivos especificados.
2. **Iteraciones de desarrollo:**
   - Como se ha comentado se seguirán ciclos iterativos de cara a la implementación y se realizarán entregas incrementales.
   - Enfoque en el desarrollo de modelos de confianza y métricas, adaptando la implementación según los hallazgos y problemas encontrados.
3. **Evaluación continua mediante simulaciones:**
   - Evaluación continua de las implementaciones parciales en entornos simulados.
   - Recopilación y análisis constante de métricas y resultados obtenidos.
4. **Retroalimentación y ajustes:**
   - Retroalimentación regular de tutores y profesores.
   - Ajuste de los modelos y métricas en función de la retroalimentación recibida.
5. **Integración de resultados:**
   - Integración final de los modelos y métricas desarrollados, teniendo en cuenta todos los ajustes y mejoras realizadas durante el proceso.
6. **Documentación:**
   - Elaboración continua de la documentación, garantizando que esté a la par con el progreso del desarrollo y las evaluaciones realizadas.

FASES DE TRABAJO:

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

Investigación bibliográfica (Semana 1-2):

- Investigación y revisión del estado del arte en seguridad y modelos de confianza en IoT.

Definición de modelos y métricas (Semana 3-5):

- Diseño y definición detallada de modelos de confianza y métricas específicas.

Desarrollo de software (Semana 6-10):

- Implementación del código en Java, integrando el protocolo MQTT y funcionalidades específicas para la simulación.

Simulación y evaluación (Semana 11-14):

- Utilización de entornos simulados para evaluar los modelos.
- Análisis de resultados y ajuste del software según sea necesario.

Documentación (Semana 15-16):

- Elaboración de la documentación del TFG, incluyendo la redacción de informes y la preparación de la presentación.

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** *Diego González Rodríguez*
Investigación bibliográfica	**53**
Definición de modelos y métricas	**70**
Desarrollo del software	**70**
Simulación y evaluación	**50**
Documentación	**53**
	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.

Lenguaje de programación:

- Java: se utilizará como el lenguaje principal para el desarrollo del código.

Protocolo de comunicación:

- MQTT (Message Queuing Telemetry Transport): se empleará para la comunicación entre dispositivos en entornos de IoT.

Hardware (Simulación):

- Arduino/Raspberry Pi: si se opta por la simulación mediante placas Arduino/Raspberry Pi, se utilizarán para emular dispositivos en un entorno de IoT.

Software de simulación (Alternativa):

- (Aún por determinar): si se decide no utilizar placas Arduino/Raspberry Pi, se elegirá un software de simulación de entornos IoT para realizar pruebas y evaluaciones.

Entorno de Desarrollo Integrado (IDE):

- Eclipse, IntelliJ u otro IDE de preferencia para el desarrollo en Java.

Gestión de Versiones:

- Git: Para control de versiones y colaboración en el desarrollo.

Documentación:

- Markdown / LaTeX / Microsoft Word: Para la redacción del informe técnico y documentación.
- Plataforma de colaboración (por ejemplo, GitHub): Para compartir y colaborar en el código fuente y otros documentos del proyecto.

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.

Placas de Desarrollo Arduino/Raspberry Pi: Empleadas para la simulación de entornos IoT, permitiendo la conexión y comunicación entre dispositivos.

Sensores IoT: Sensores u otros dispositivos que reproduzcan las condiciones del mundo real para evaluar la confianza y obtener datos.

Dispositivos IoT Comerciales: Integración de dispositivos reales presentes en hogares inteligentes para pruebas específicas.

Java: Lenguaje de programación principal para el desarrollo del software de evaluación de confianza entre dispositivos.

Protocolo MQTT: Utilizado para la comunicación entre dispositivos en el entorno simulado.

Entornos de Simulación: Software de simulación que reproduce las complejidades del mundo real para realizar pruebas controladas.

IDE (Entorno de Desarrollo Integrado): Herramientas de desarrollo como Eclipse, IntelliJ o VSCode para la codificación y depuración del software.
Markdown / LaTeX / Microsoft Word: Para la redacción del informe técnico y documentación.
Documentación y Colaboración: Plataformas como Google Docs o herramientas de control de versiones (Git) para la documentación y colaboración en el código.
Jira, Trello u otras herramientas de gestión de proyectos para organizar y seguir el progreso de las tareas.
Plataforma de Comunicación: herramientas como Gmail o Microsoft Teams para facilitar la comunicación y colaboración con los profesores y tutores.

REFERENCIAS

Listado de referencias (libros, páginas web, etc.)

Ferraris, D., Fernandez-Gago, C., Roman, R., & Lopez, J. (2023). A survey on IoT trust model frameworks. The Journal of Supercomputing, 1-38.

Ferraris, D., Fernandez-Gago, C., Daniel, J., & Lopez, J. (2019, January). A segregated architecture for a trust-based network of internet of things. In 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC) (pp. 1-6). IEEE.

La Marra, A., Martinelli, F., Mori, P., Rizos, A., & Saracino, A. (2018). Introducing usage control in MQTT. In Computer Security: ESORICS 2017 International Workshops, CyberICPS 2017 and SECPRE 2017, Oslo, Norway, September 14-15, 2017, Revised Selected Papers 3 (pp. 35-43). Springer International Publishing.

La Marra, A., Martinelli, F., Mori, P., & Saracino, A. (2017, August). Implementing usage control in internet of things: a smart home use case. In 2017 IEEE Trustcom/BigDataSE/ICESS (pp. 1056-1063). IEEE.

Chen, L., Vidalis, S., & Yang, S. (2023, August). A Trust-Based Approach for Data Sharing in the MQTT Environment. In 2023 20th Annual International Conference on Privacy, Security and Trust (PST) (pp. 1-5). IEEE.

Fernandez-Gago, C., Moyano, F., & Lopez, J. (2017). Modelling trust dynamics in the Internet of Things. Information Sciences, 396, 72-82.

Málaga, 29 de Febrero de 2024

Firma tutor/tutora:

FERNANDEZ GAGO MARIA DEL CARMEN - 25667073Q
Firmado digitalmente por FERNANDEZ GAGO MARIA DEL CARMEN - 25667073Q
Fecha: 2024.02.29 18:10:07 +01'00'

Firma cotutor/a:

FERRARIS DAVIDE - Y5040871K
Firmado digitalmente por FERRARIS DAVIDE - Y5040871K
Fecha: 2024.02.29 10:37:48 +01'00'

Firma tutor/a coordinador/a: