media/image1.jpg

Plataforma segura de actualizaciones para dispositivos IoT

TRABAJO DE FIN DE MÁSTER PRESENTADO EN: Escuela Politécnica Superior de Mondragon Unibertsitatea

AUTOR/A: Nombres de los autores

DIRECTOR/A: .....
TUTOR/A: .....

CURSO ACADÉMICO: 2024/2025

Resumen

El Trabajo de Fin de Máster propone el diseño, implementación y evaluación de una plataforma de actualización remota (OTA) segura y escalable para dispositivos IoT. La motivación principal radica en la elevada cantidad de dispositivos que sufren por vulnerabilidades y la falta de actualizaciones para solucionarlas, lo que crea vectores de ataque a gran escala. Esta plataforma permite la distribución de actualizaciones firmadas y cifradas a flotas de dispositivos para garantizar la autenticidad, integridad y confidencialidad del software desplegado.

Para cubrir tanto dispositivos con recursos limitados como escenarios que requieren resistencia ante futuros ataques cuánticos, el sistema proporciona soporte para dos familias de algoritmos criptográficos: algoritmos de cifrado y firma con resistencia post-cuántica, y algoritmos de criptografía ligera (lightweight cryptography) optimizados para dispositivos con restricciones de memoria, CPU y energía.

El trabajo incluye un análisis del estado de la práctica sobre actualizaciones OTA en IoT y de las necesidades de seguridad actuales, mostrando la importancia de incorporar criptografía ligera para dispositivos con recursos limitados y la opción de soluciones resistentes a la computación cuántica cuando el contexto lo requiera. Además, se desarrolla un prototipo de plataforma, desplegable en la nube y diseñado para escalar horizontalmente, que se prueba en un banco de dispositivos heterogéneos.

extbfPalabras claves: OTA, IoT, actualizaciones seguras, post-cuántico, criptografía ligera, firma digital, cifrado.

Impacto en los Objetivos de Desarrollo Sostenible (ODS): xxx, xxx, xxx, xxx.

Laburpena

Idatzi laburpena hemen.

Hitz gakoak: xxx, xxx, xxx, xxx.

Garapen Jasangarriko Helburuetan (GJH) eragina: xxx, xxx, xxx, xxx.

Abstract

This Master's thesis proposes the design, implementation and evaluation of a secure and scalable over-the-air (OTA) update platform for IoT devices. The platform targets the large number of vulnerable devices that remain unpatched and provides mechanisms for signed and encrypted updates. It supports both post-quantum cryptography and lightweight cryptography to accommodate different device capabilities. The thesis also analyzes current OTA practices and demonstrates the need for lightweight cryptography as well as the optional use of post-quantum primitives when required. A cloud-deployable, horizontally scalable prototype is developed and tested across heterogeneous devices, with an experimental evaluation measuring update latency, resource usage, success rates and energy consumption.

extbfKeywords: OTA, IoT, secure updates, post-quantum, lightweight cryptography, digital signatures, encryption.

Sustainable Development Goals (SDG) impact: xxx, xxx, xxx, xxx.

Agradecimientos

A las empresas que han subvencionado este trabajo.

A los que han revisado este documento.

A los que me han proporcionado información.

NOTA. Escribir aquí los agradecimientos y, si no se va a usar, borrar la página.

Índice de contenidos

Índice de Figuras

NOTA. Introducir el Índice de Figuras. Recuerda también referenciar las figuras si no son propias. Incluir materiales ajenos suele conllevar la petición de derechos para su uso

Índice de Tablas

NOTA. Introducir el Índice de Tablas, en caso de utilizarlas en la memoria. Recuerda también referenciar las tablas si no son propias. Incluir materiales ajenos suele conllevar la petición de derechos para su uso.

Símbolos y abreviaturas

ODS Objetivos de Desarrollo Sostenible

TFM Trabajo Fin de Máster

NOTA. Introducir los símbolos y abreviaturas utilizadas en la memoria.

Introducción

La introducción ha de aclarar qué tipo de documento es el entregado, qué representa, cuál es el trabajo desarrollado que se incluye en él, qué apartados, su importancia y qué aporta.

Este documento integra una orientación sobre la preparación del Trabajo Fin de Grado (TFG), Trabajo Fin de Máster (TFM) de Ingeniería realizada en la Escuela Politécnica Superior de Mondragon Unibertsitatea

[1].

En el documento encontrará ejemplos para el formato y la presentación de los resultados, así como para la organización de los capítulos del TFG/TFM y su contenido. Este documento se puede utilizar como una plantilla para la composición de la propia memoria

[2,3]. La forma, en la preparación de la memoria no es menos importante que el contenido. Por lo tanto, debe poner el máximo interés y respeto por la gramática y la sintaxis de la lengua en la que ésta se redacte.

En cuanto a la elección del pronombre personal con el que se expresen, se recomienda que el uso del pronombre impersonal, incluso en combinación con la primera persona del singular. En beneficio de la claridad, es aconsejable evitar frases largas, el uso frecuente de cursiva, negrita y subrayado en el texto.

Problemática

El objetivo es explicar y delimitar de forma clara y precisa el problema que abordará el proyecto.

Se debe seleccionar y relacionar la temática del proyecto con las competencias del perfil de ingeniería en el que se enmarca.

Antecedentes

El apartado de antecedentes puede ser opcional, dependerá del tipo de proyecto, en función de si el proyecto ha tenido fases previas o forma parte de un proyecto mayor, etc.

Estado del arte

El apartado del estado del arte requiere aportar la situación en la comunidad científica o en el mercado de la tecnología, la metodología o los productos técnico-tecnológicos afectados (incluir citas en el texto, las cuales, incluyen algún conocimiento de vanguardia de su especialidad de ingeniería).

Objetivos

Se deben establecer objetivos claros, Medibles, Alcanzables, Retadores, Temporalizados y Específicos MARTE/SMART (Specific, Measurable, Achievable, Realistic and Time-bound)[1]., alineándolos con los siguientes elementos: impacto social, seguridad y salud, sostenibilidad medioambiental, económico e industrial.

Incluir, tanto los objetivos del proyecto técnico, como los objetivos de aprendizaje.

Planificación del Proyecto

Se identifican las actividades, hitos, entregables, recursos necesarios, personas responsables y tiempos del proyecto. Se suele representar a través de un diagrama de Gantt.

Pliego de condiciones

El pliego de condiciones ha de recoger recursos, requisitos, condiciones específicas y normas y reglamentos (normas UNE) necesarios para la realización del proyecto.

Desarrollo

El desarrollo se estructura en capítulos en los que se abordan los diferentes temas del trabajo. Los capítulos han de tener títulos representativos de su contenido, su número es variable y se subdividen en epígrafes.

Tener en cuenta los siguientes aspectos:

-> El marco teórico, las técnicas y métodos de análisis, diseño e investigación aplicados y sus limitaciones.

->Las destrezas prácticas aplicadas para la resolución de problemas complejos, la realización de diseños de ingeniería complejos y la realización de investigaciones.

->Los materiales, equipamiento y herramientas aplicados, así como las tecnologías y procesos de ingeniería aplicados; y sus respectivas limitaciones dentro de su ámbito de especialidad.

->La aplicación de las normas asociadas a la práctica.

[1] https://www.mindtools.com/pages/article/smart-goals.htm

Teoría/cálculos

Opcional. Utilizar este apartado si procede. Si se aporta alguna novedad en relación con los artículos citados en la introducción, ésta debe desarrollarse en esta sección, no hay que repetir lo que ya está publicado.

Los cálculos deben desarrollarse a partir de la base teórica citada o presentada.

Resultados

Se presentan los logros del proyecto. Los datos comúnmente se presentan en formato de tablas, cuadros, gráficos u otras figuras explicando su significado.

Discusión

A veces es apropiado poner los resultados y la correspondiente discusión en una misma sección. Debe explorar el significado de los resultados del trabajo, no repetirlos. Evitar demasiadas citas y discusiones en torno a la literatura publicada.

Memoria económica

Analiza la viabilidad económica del Proyecto. Ha de contemplar el análisis de coste de materiales, horas de dedicación, inversiones, costes de explotación, financiación, retorno de la inversión, etc.

Conclusiones

Relacionar los resultados del proyecto con los objetivos, es decir, aportando conclusiones de aspectos técnicos, metodológicas, de salud y seguridad laboral, económicas, relativas al impacto en los Objetivos de Desarrollo Sostenible (ODS).

Líneas futuras

El apartado de Líneas futuras debe expresar las ideas o los estudios que se podrían llevar a cabo para ampliar o mejorar los resultados obtenidos. Podría ser el punto de partida para la continuación del trabajo realizado en el proyecto.

Valoración personal

Identificación de las aportaciones, lo que ha supuesto el TFM en materia de aprendizaje. Valoración de las tareas desarrolladas y los conocimientos y competencias adquiridos en relación con los estudios universitarios

Bibliografía

Todo trabajo académico y de investigación necesita estar documentado. Para ello es necesario consultar información ya disponible en obras ajenas (artículos, libros, webs, normas técnicas, prensa, informes...). Toda esta información consultada conforma la base bibliográfica de tu propio trabajo y debe aparecer reflejada en citas, referencias bibliográficas y en la bibliografía[2].

Se recomienda utilizar aplicaciones de gestión de referencias bibliográficas como Mendeley O Zotero. Importante insertar y vincular adecuadamente las citas bibliográficas y la bibliografía en la memoria.

Se incluyen los enlaces a los programas citados y a los plugins para crear citas y bibliografía automáticamente en los programas de texto como Word:

Mendeley https://www.mendeley.com/

Citar con Mendeley: Cite https://www.mendeley.com/reference-management/mendeley-cite

Zotero https://www.zotero.org/

Citar con Zotero https://www.zotero.org/download (Los plugin para Word etc. se instalan junto con Zotero en el pc)

Se incluye un breve ejemplo de referencias (pueden utilizarse otros formatos más afines a la titulación).

[1] C. Vogt (1999). Creating Long Documents using Microsoft Word, Published Web University Waterloo.

[2] J.L. Caivano (1995). Guía para realizar, escribir y publicar trabajos de investigación.

[3] M. Corcelles, M. Cano, G.B. Faz, N. Vega (2013)., Enseñar a escribir textos científico-académicos mediante la revisión colaborativa. REDU Revista Docencia Universitaria.

[4] Asociación Española de Normalización y Certificación (1991). Cables para aparatos de elevación: Criterios de examen y de sustitución de los cables. AENOR. Norma UNE 157001, 2014

[5] Robinson, A., & Stern, S. (1998). Corporate creativity: how innovation and improvement actually happen. Berrett Koehler. ISBN 1-57675-049-3.

[6] Kramer, M.S. [et al.]. (2001). Promotion of Breastfeeding Intervention Trial [en línea]. JAMA. January 24/31, vol. 285, No. 4. http://jama.jamanetwork.com/article.aspx?articleid=193490

[2] https://mondragon.libguides.com/como-redactar-citas-referencias-bibliografia

Índice alfabético

Opcional. En los libros y en las tesis doctorales además de la tabla de contenidos, los índices de tablas y figuras, es muy habitual encontrarse con un índice alfabético donde se listan palabras claves y la página correspondiente en la que dichas palabras están citadas.

En general el índice alfabético se coloca al final del documento después de la Bibliografía.

Capítulo de muestra

NOTA: Eliminar este capítulo de la versión definitiva.

En este capítulo hay un texto de muestra que incluye ecuaciones, gráficos y una tabla.

La mecánica (o mecánica clásica) es la rama principal de la llamada Física Clásica, dedicada al estudio de los movimientos y estados en que se encuentran los cuerpos. Describe y predice las condiciones de reposo y movimiento debido a la acción de las fuerzas.

Se divide en tres partes:

- *Cinemática:* Estudia las diferentes clases de movimiento de los cuerpos sin atender a las causas que lo producen.
- *Dinámica:* Estudia los efectos de la interacción entre un sistema con su entorno, sobre su estado de movimiento.
- *Estática:* está comprendida dentro del estudio de la *dinámica* y analiza las condiciones que permiten el equilibrio de los cuerpos.

Cinemática

La cinemática es una rama de la física dedicada al estudio del movimiento de los cuerpos en el espacio, sin atender a las causas que lo producen (lo que llamamos fuerzas). Por tanto, la cinemática sólo estudia el movimiento en sí, a diferencia de la dinámica que estudia las interacciones que lo producen. El Análisis Vectorial es la herramienta matemática más adecuada para ellos.

En cinemática distinguimos las siguientes partes:

- Cinemática de la partícula
- Cinemática del sólido rígido

La magnitud vectorial de la Cinemática fundamental es el "desplazamiento" s, que experimenta un cuerpo durante un lapso t. Como el desplazamiento es un vector, por consiguiente, sigue la ley del paralelogramo, o la ley de suma vectorial. Así si un cuerpo realiza un desplazamiento "consecutivo" o "al mismo tiempo"

dos desplazamientos 'a' y 'b', nos da un deslazamiento igual a la suma vectorial de 'a' + 'b' como un solo desplazamiento como se ilustra en la Figura 2.

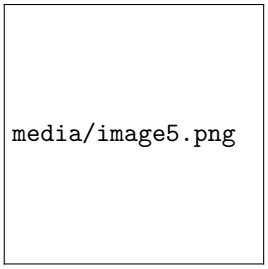

Figura 1 Suma de dos vectores

Dos movimientos al mismo tiempo entran principalmente, cuando un cuerpo se mueve respecto a un sistema de referencia y ese sistema de referencia se mueve relativamente a otro sistema de referencia.

Ejemplo: El movimiento de un viajero en un tren en movimiento, que está siendo visto por un observador desde el terraplén. O cuando uno viaja en coche y observa las montañas y los árboles a su alrededor.

Rapidez y aceleración

Diariamente escuchamos los conceptos de rapidez y aceleración como velocidad y aceleración solamente. Pero en física la velocidad y la aceleración son vectores, por lo que es claro y necesario su diferenciación y entendimiento. De aquí en adelante (más por costumbre que por ganas) llamaremos tanto a la rapidez y a la aceleración solamente como velocidad y aceleración (a menos que se especifique lo contrario).

Si cubre una masa puntual en un punto P en un tiempo t el tramo s, se llamará al cociente s/t su velocidad media v_m en el intervalo de tiempo t o en el tramo s.

Se observa que s aquí no es el desplazamiento, sino la longitud de arco: es el camino recorrido.

La llamamos velocidad media porque la masa puntual no se mueve por el trayecto uniforme trazado. O sea, estamos tomando sólo los puntos final e inicial para hacer los cálculos.

Hagamos el trayecto como s (de manera diferencial, o sea infinitesimal), al igual que al intervalo de tiempo t. Para s cercano a cero (o t cercano a cero, que tienda a cero) el cociente s/t como valor al límite, nos da la velocidad v de la masa puntual en el punto P. En el análisis se puede calcular ese valor al límite también como $\mathrm{d}s/\mathrm{d}t$.

Tomemos luego una masa puntual que tiene en el punto P y en el tiempo t la velocidad v; y en el tiempo $t + t$ y la velocidad $v + \mathbf{v}$. Podemos calcular el cociente v/t como la aceleración media de la masa puntual en el intervalo de

tiempo t. Para t cercano a cero se aspira a que ese cociente tenga un valor límite, la aceleración a de la masa puntual para el tiempo t.

Es el camino descrito como una función analítica del tiempo t, así $s{=}s(t)$, la función de velocidad $v(t)$ es la primera derivada de la función $s(t)$ con respecto al tiempo, la función de aceleración $a(t)$ es la segunda derivada. La derivación con respecto al tiempo se puede también escribir como un punto sobre las variables. En sentido contrario se puede encontrar la función de velocidad y la función de la trayectoria a través de la integración como se expresa en (12.1)

$$v(t) = \int a(t)\ dt \qquad s(t) = \int v(t)\ dt = \iint a(t)\ dt\ dt \tag{12.1}$$

Ejemplo: En caída libre una masa puntual se encuentra con una aceleración constante g. Esto es, cuando el tiempo $t{=}0$ verticalmente de arriba hacia abajo, tiene la velocidad y sus coordenadas como se expresa en (12.2).

$$v(t) = g \int dt = g\ t + \ v_0 \qquad s(t) = \int (g\ t + \ v_0)\ dt = \frac{1}{2} g\ t^2 + v_0 t + s_0 \tag{12.2}$$

En la Tabla 1 se ve bla bla.

Tabla 1 Elementos geométricos

Elemento	**Descripción**	**Imagen**
Baricentro	El baricentro o centroide de una superficie plana donde cada circunferencia une un punto con otros contenida en una figura geométrica plana, es un punto tal, que cualquier recta que pasa por él, divide a dicha superficie en dos partes de igual momento respecto a dicha recta.	media/image6.png
Centroide	El centroide es un concepto puramente geométrico que depende de la forma del sistema; el centro de masas depende de la distribución de materia, mientras que el centro de gravedad depende también del campo gravitatorio.	media/image7.png

Anexos

Los Anexos han de identificare con letras o números. Las fórmulas tablas y figuras de los anexos tienen numeración propia (A-1), (B-1)....

Anexos

Podemos numerar las figuras como se ilustra en la Figura A-1:

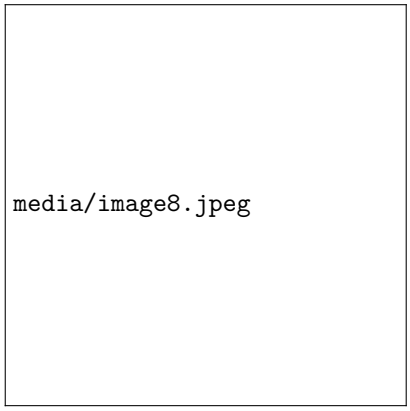

Figura A-1 Figura del anexo A

Cálculos de resistencia