Universidad de La Laguna

Máster Universitario en Ciberseguridad e Inteligencia de Datos

Detección de somnolencia en conductores con un reloj inteligente

Drowsiness detection in drivers with a smartwatch

Sonia Díaz Santos

La Laguna, 7 de Septiembre de 2022

D. **Pino Caballero Gil**, con N.I.F. 45.534.310-Z Catedrática de Universidad adscrita al Departamento de Ingeniería Informática y de Sistemas de la Universidad de La Laguna, como tutora

D. **Yanira González González**, con N.I.F. 78.555.933-P Técnico titulado Medio en informática en el HUC, como cotutora

C E R T I F I C A (N)

Que la presente memoria titulada:

"Detección de somnolencia en conductores con un reloj inteligente"

ha sido realizada bajo su dirección por D. **Sonia Díaz Santos**, con N.I.F. 42.237.482-Y.

Y para que así conste, en cumplimiento de la legislación vigente y a los efectos oportunos firman la presente en La Laguna a 7 de Septiembre de 2022.

Agradecimientos

En primer lugar agradecer tanto a mi tutora, Pino Caballero Gil, como a mi cotutora, Yanira González González, por su ayuda, orientación y apoyo durante la realización de este proyecto.

Así como a la empresa Nokia Spain SA, por permitirme participar en el desarrollo del proyecto IMMINENCE.

También agradecer a mi familia, amigos y compañeros que me han ayudado y apoyado a lo largo de estos meses de trabajo.

Licencia

Resumen

El objetivo principal de este trabajo es recopilar información acerca de las variables fisiológicas más significativas de una persona mientras se encuentra conduciendo a través de un reloj inteligente. Con los datos obtenidos se detecta si la persona que conduce presenta síntomas de sueño y, por lo tanto, se está quedando dormido. La finalidad es generar una alerta produciendo una vibración en el reloj para despertar al sujeto si este está adormecido o fatigado. Asimismo, para dar solución a este proyecto es necesario detectar la acción de conducción. De este modo se consigue reducir el número de accidentes por somnolencia, evitando daños tanto materiales como humanos.

Palabras clave: reloj inteligente, seguridad vial, somnolencia, variables fisiológicas, conducción segura, programación segura

Abstract

The main objective of this work is to detect early if a driver shows symptoms of sleepiness that indicate that he/she is falling asleep and, in that case, generate an alert to wake him/her up. To solve this problem, an application has been designed that collects various parameters, through a smartwatch while driving. First, the application detects the driving action. Then, it collects information about the most significant physiological variables of a person while driving. On the other hand, given the high level of sensitivity of the data managed in the designed application, in this work special attention has been paid to the security of the implementation. The proposed solution improves road safety, reducing the number of accidents caused by drowsiness while driving.

Keywords: road safety, smartwatch, drowsiness, physiological variables, safe driving, safe scheduling

Índice general

Índice de figuras

Capítulo 1 Introducción

Los accidentes de tráfico a menudo ponen en peligro la vida no solo de quien conduce sino también de otras personas en la carretera. Por lo tanto, es necesario hacer todo lo posible para reducir este número. Entre las opciones para lograrlo, este trabajo ha optado por el desarrollo de tecnologías innovadoras para abordar el problema. En concreto, el presente estudio se ha centrado en identificar variables fisiológicas que caracterizan la somnolencia o la fatiga durante la conducción, con el objetivo de utilizarlas para reducir el número de accidentes provocados por ese motivo, ya que, en general, la somnolencia está implicada, directa o indirectamente, en el 15-30% de los accidentes de tráfico [1].

En este trabajo se ha realizado un estudio de las variables fisiológicas más relevantes que permiten concluir si una persona se está quedando dormida. Según diversas publicaciones, estas variables son: frecuencia cardíaca, electrocardiograma, función respiratoria y estrés. En concreto, mediante el reloj inteligente utilizado en este trabajo se han podido recoger los datos de estas variables fisiológicas de una persona, localizar los signos de somnolencia y comprobar, en tiempo real, si la persona se está quedando dormida [2].

Por otro lado, para detectar la acción de conducir, el reloj inteligente cuenta con un conjunto de sensores como acelerómetro, giroscopio, podómetro y GPS (GPS, Global Positioning System).

Así, este trabajo parte de la intersección entre la lista de variables fisiológicas descriptivas del sueño y la de los sensores disponibles en el reloj inteligente utilizado. En particular, se han usado algunos parámetros como la Variabilidad de la Frecuencia Cardíaca (VFC). Luego, estos datos recopilados se han analizado para detectar la somnolencia en las personas que conducen. Para ello se han utilizado diferentes sensores: PPG (PPG, PhotoPlethysmoGraphy) y ECG (ECG, ElectroCardioGram). El sensor PPG utiliza una tecnología basada en la luz para detectar la tasa de flujo sanguíneo controlada por la acción de bombeo del corazón. Además, para monitorizar la actividad física de la persona se han usado otros sensores como el acelerómetro, giroscopio, podómetro y GPS, integrados en el reloj [3].

También se han tenido en cuenta otros factores, como la hora del día o ritmo circadiano según el cual se producen cambios físicos, mentales y de comportamiento en ciclos de 24 horas. De hecho, se sabe que los accidentes relacionados con la fatiga dependen en gran medida de la hora del día, así como del tipo de carretera, especialmente en carreteras monótonas. Además, otros factores a considerar son la edad de la persona, el género y la práctica regular de ejercicio físico, para determinar los parámetros normales de cada

individuo. Por ejemplo, la frecuencia cardíaca en los deportistas suele ser más baja que en las personas sedentarias, y la frecuencia cardíaca suele ser más baja en las mujeres que en los hombres. Teniendo en cuenta todos estos indicadores, ha sido posible un mejor análisis de los datos de somnolencia [4].

Este documento está estructurado de la siguiente manera. La sección 2 proporciona datos del reloj inteligente y la plataforma utilizada. La Sección 3 contiene una discusión de variables fisiológicas y sensores de interés para este trabajo. La Sección 4 proporciona una descripción del diseño y las funcionalidades de la aplicación propuesta. La Sección 5 describe algunas características de la implementación segura de la aplicación. Finalmente, las secciones 6 y 7 cierran el trabajo con algunas conclusiones y trabajo futuro.

Capítulo 2 Reloj inteligente y plataformas utilizadas

Esta sección proporciona algunos detalles del reloj inteligente escogido para medir los datos de la persona que conduce, así como de la plataforma utilizada para desarrollar las aplicaciones [5].

2.1 Hardware

Para el desarrollo de este trabajo se ha usado el reloj inteligente Samsung Galaxy Watch 4 LTE (LTE, Long Term Evolution). Este reloj cuenta con el *Wear OS Powered by Samsung*, que permite monitorear la salud las 24 horas del día. Dispone de un sensor *BioActive* que mide el ECG y la tensión arterial en tiempo real. Para medir la presión arterial utiliza un sensor óptico de frecuencia cardíaca PPG y para el ECG un sensor cardíaco eléctrico. También permite medir la composición corporal a través del sensor de análisis de impedancia bioeléctrica (BIA, Bioelectrical Impedance Analysis). Este dispositivo puede medir los niveles de estrés y oxígeno en sangre para obtener un análisis completo del sueño. Dispone de dos sensores de movimiento, el acelerómetro y el giroscopio, para conocer la ubicación con el sensor GPS, y calcula los pasos con el sensor podómetro. En cuanto a las conexiones, cuenta con Bluetooth 5.0 y conexión Wi-Fi [6].

2.2 Software

Esta sección define el software utilizado por los dispositivos, incluida la arquitectura de comunicación entre los sistemas, así como las tecnologías y los entornos de desarrollo. También habla acerca de la plataforma *Health* y la comunidad *Wear OS*.

2.2.1 Esquema de comunicación de la arquitectura

Se requieren conexiones Bluetooth o Wi-Fi para la comunicación entre los diferentes dispositivos, como se muestra en la Figura 2.2.1. El reloj inteligente con *Wear OS Powered by Samsung* tiene una conexión Bluetooth para conectarse al teléfono móvil. El móvil cuenta con la aplicación *Samsung Health*, que recolecta los datos necesarios de variables fisiológicas, así como la aplicación *Samsung Health Monitor* para obtener los datos de la presión arterial y electrocardiograma de la persona que usa el reloj. La aplicación se crea en el ordenador y se instala en el móvil a través del entorno de desarrollo Android Studio.

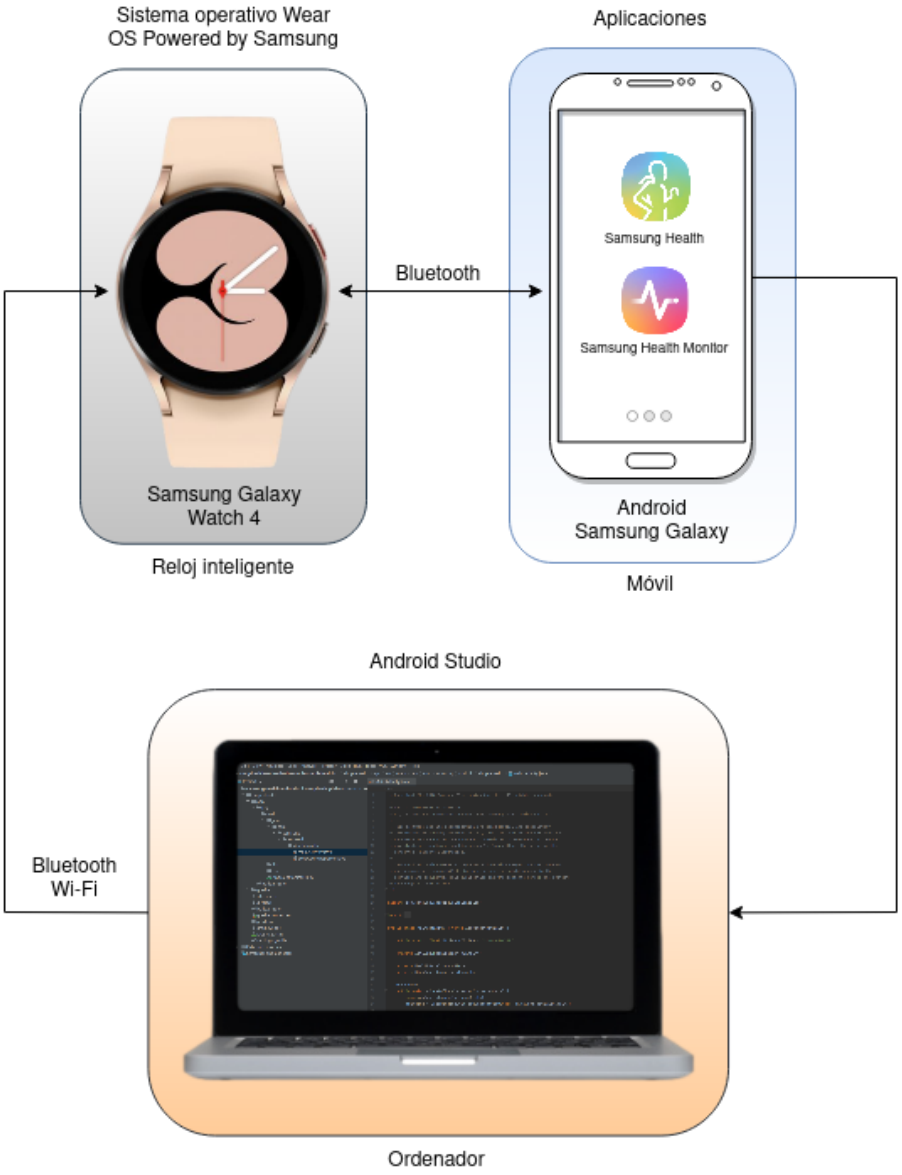

Figura 2.2.1. Esquema de comunicación de la arquitectura

2.2.2 Tecnologías

Las tecnologías utilizadas incluyen la herramienta Android Studio para desarrollar la aplicación. Los lenguajes de programación que se pueden utilizar para llevarlo a cabo son Kotlin y Java. Es necesario tener las aplicaciones en el móvil para tener acceso a los datos de quien conduce y realizar su análisis con el fin de detectar si la persona está conduciendo y presenta síntomas de somnolencia.

2.2.3 Plataforma *Health*

El kit de desarrollo de software (SDK, Software Development Kit) de Samsung Health para Android permite compartir datos de salud entre Samsung

Health, que se ejecuta en teléfonos Android, y aplicaciones de terceros, como se muestra en la Figura 2.2.3. También permite que las aplicaciones de terceros utilicen la función de seguimiento de Samsung Health mediante la creación de aplicaciones con el SDK. El SDK proporciona acceso seguro a los datos de Samsung Health con los tipos de datos aplicables. Sin embargo, el intercambio de datos solo está habilitado después del consentimiento explícito del usuario. El usuario puede seleccionar configuraciones detalladas para compartir datos, incluida la aplicación asociada que accederá a los datos del usuario y qué tipo de datos se leerán o escribirán.

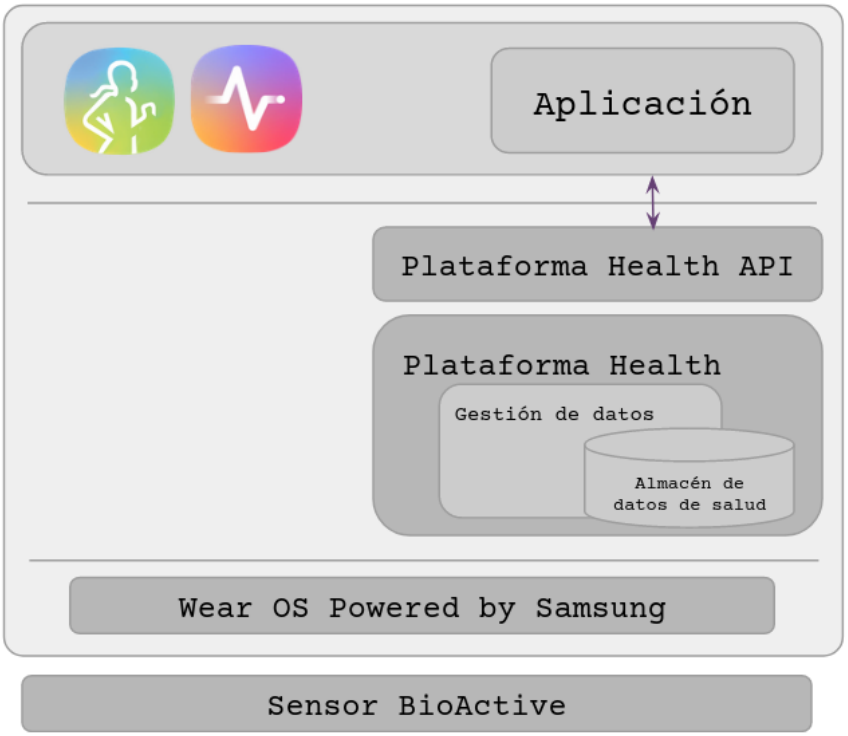

Figura 2.2.3. Plataforma *Health*

2.2.4 Comunidad *Wear OS*

La comunidad *Wear OS Powered by Samsung* tiene una plataforma dedicada para desarrolladores de Android con una multitud de tutoriales sobre cualquier tipo de dispositivo Android. Hay comunidades en YouTube: Desarrolladores de Android, en Twitter: AndroidDev y en LinkedIn: Desarrolladores de Android.

2.3 Compatibilidad

La compatibilidad entre dispositivos para tener una funcionalidad completa y acceso a todos los datos es compleja. El reloj inteligente Samsung Galaxy Watch 4 es compatible con cualquier dispositivo Android, pero para obtener los datos de los sensores de ECG y presión arterial, el teléfono móvil debe ser un

Samsung Galaxy con una versión de Android superior a N, una capacidad de memoria RAM de al menos al menos 1,5 Gb y tener los servicios de Google para móviles (GMS, Google Mobile Services). Esto significa que aunque la aplicación Samsung Health es compatible con dispositivos Android, incluidos dispositivos que no sean Samsung, si desea obtener esos datos fisiológicos e instalar la aplicación Samsung Health Monitor, las restricciones cambian.

Capítulo 3 Sensores y variables fisiológicas

Esta sección detalla cómo se ven influenciadas las variables fisiológicas más relevantes para este trabajo y cómo funcionan los sensores utilizados para recopilar los datos [7].

3.1 Fases del sueño

La Figura 3.1 muestra el esquema de las fases del sueño, en las que la somnolencia inicial es la más relevante para este trabajo. La fase 1 es el grado más ligero de sueño y dura unos minutos. En esta fase, la actividad fisiológica disminuye con una caída gradual de los signos vitales y del metabolismo. En esta fase es fácil que los estímulos sensoriales despierten a una persona.

Durante el sueño no sólo se producen los cambios más conocidos, como alteraciones del electroencefalograma (EEG, ElectroEncephaloGraphy), movimientos rápidos de los ojos(REM, Rapid Eye Movements) o alteraciones del tono muscular evaluadas con electromiografía (EMG, ElectroMyoGraphy), sino también importantes alteraciones cardiovasculares, respiratorias, hormonales, renales, cambios digestivos y generales de todo el organismo. La presión arterial, el pulso y la función respiratoria están disminuidos.

Figura 3.1. Fases del sueño

3.2 Detección de sueño y conducción

Para detectar el sueño se recopilan datos sobre las siguientes variables fisiológicas: frecuencia cardíaca, estrés, presión arterial y oxígeno en sangre [8].

La frecuencia cardíaca en reposo es el número de veces que el corazón late por minuto cuando está en reposo. Una frecuencia cardíaca baja en reposo

suele ser sinónimo de buena salud cardiovascular. El ejercicio aeróbico puede ayudar a reducir la frecuencia cardíaca en reposo con el tiempo. La temperatura, la posición del cuerpo, la actividad reciente o el estado emocional son algunos de los factores que pueden afectar a la frecuencia cardíaca.

El estrés se mide con ciertos biomarcadores. Cuanto mayor sea el número de mediciones realizadas, mayor será la precisión de los datos de tensión recopilados. El tabaco, el alcohol, la cafeína y los medicamentos pueden afectar a las mediciones del nivel de estrés. Al usar la función de nivel de estrés, los relojes usan datos de frecuencia cardíaca, como latidos por minuto, para determinar el intervalo entre cada latido. Una menor variabilidad entre latidos equivale a mayores niveles de estrés, mientras que una mayor variabilidad indica menos estrés.

La presión arterial se mide mediante un sensor óptico de frecuencia cardíaca conocido como sensor PPG. Controlar la presión arterial es muy importante para la salud. Si la presión arterial está dentro del rango normal, es una buena indicación de que se tiene un corazón sano. Pero tener presión arterial alta, también conocida como hipertensión, puede aumentar significativamente el riesgo de enfermedades cerebrales, renales y cardíacas, incluidos los accidentes cerebrovasculares y las enfermedades coronarias, cuando no se controlan adecuadamente. En la aplicación se clasifican en: pulso, presión arterial sistólica y presión arterial diastólica. El rango de medición para lecturas de presión arterial es: sistólica: 70-180 y diastólica: 40-120.

El nivel de oxígeno en la sangre es un indicador de cuán eficientemente se transporta el oxígeno a través del cuerpo, lo que a su vez indica si está respirando de manera eficiente. El nivel de oxígeno en sangre, también conocido como saturación de oxígeno percutánea (SpO2, Saturation of Peripheral Oxygen), es la medida del porcentaje de hemoglobina que se oxigena en los glóbulos rojos. Un rango saludable es 95-100% cuando está en reposo. Factores como el ejercicio intenso, la cantidad de oxígeno en el aire, la altitud y varios problemas de salud pueden dar lecturas porcentuales más bajas [9], [10].

Todos estos datos son recopilados por el sensor *Samsung BioActive*, que es un sensor de un solo chip 3 en 1. Los sensores son: PPG, ECG y BIA.

El sensor PPG es capaz de medir la frecuencia cardíaca, el oxígeno en sangre, el nivel de estrés y la frecuencia respiratoria. Foto significa luz, Pletismógrafo significa cambio de volumen y Gram significa gráfico. Por lo tanto, PPG es un sensor de luz infrarroja verde de baja intensidad y alta precisión que se utiliza para detectar el volumen del flujo sanguíneo y comprender la fluctuación en la frecuencia cardíaca.

El sensor de ECG se utiliza para la detección del ritmo cardíaco y la frecuencia cardíaca. Dado que este sensor es voluminoso, no se puede utilizar para detectar la frecuencia cardíaca cuando el cuerpo está en movimiento. Por lo tanto, la frecuencia cardíaca y la variabilidad de la frecuencia cardíaca (VFC)

se pueden medir de forma precisa y continua, incluso durante la actividad física extrema [11], [12], [13].

Funcionalmente, cuando el corazón late, los capilares se expanden y contraen de acuerdo con los cambios en el volumen sanguíneo. El sensor óptico de PPG, que utiliza tecnología tolerante al movimiento, emite señales de luz que se reflejan en la piel para medir de manera precisa y continua las señales débiles del flujo sanguíneo. Entonces, cuando la luz viaja a través de los tejidos biológicos, es absorbida por los huesos, los pigmentos de la piel y la sangre venosa y arterial. Dado que la sangre absorbe la luz con más fuerza que los tejidos circundantes, los sensores PPG pueden detectar cambios en el flujo sanguíneo como cambios en la intensidad de la luz. La señal de voltaje de PPG es proporcional a la cantidad de sangre que fluye a través de los vasos sanguíneos. Incluso pequeños cambios en el volumen de sangre pueden detectarse con este método, proporcionando una mayor precisión.

La función de electrocardiograma funciona registrando la actividad eléctrica del corazón a través de un sensor en un *Samsung Galaxy Watch* compatible. La aplicación mide la frecuencia y el ritmo cardíaco, que se clasifican como ritmo sinusal o fibrilación auricular. Un ritmo sinusal es cuando el corazón late constantemente. Esto ocurre cuando las cámaras superior e inferior del corazón bombean sincrónicamente. La fibrilación auricular es cuando el corazón late a un ritmo irregular. Esto sucede cuando las cámaras superiores del corazón no bombean en sincronía con las cámaras inferiores. Si no se trata, puede provocar coágulos de sangre, accidentes cerebrovasculares, insuficiencia cardíaca y otros problemas de salud. Si se presentan síntomas, pueden incluir latidos cardíacos rápidos o palpitaciones, latidos salteados, fatiga, dificultad para respirar, presión o dolor en el pecho, desmayos o mareos [14].

El sensor BIA realiza análisis de composición corporal en tiempo real colocando dos dedos en los dos botones laterales, que actúan como electrodos, para medir la masa muscular, la masa grasa, la grasa corporal, el índice de masa corporal (IMC) y el agua corporal.

Para detectar la acción de conducción, se recopilan datos de los siguientes sensores: acelerómetro, giroscopio, podómetro y GPS.

El acelerómetro mide la fuerza, dirección y gravedad de la aceleración y orientación del dispositivo, como se ve en la Figura 3.2.1.

El giroscopio mide la velocidad angular del dispositivo y, por lo tanto, su posición exacta, como se muestra en la Figura 3.2.2. Al vincular los datos del giroscopio con los de otros sensores como el acelerómetro, la pulsera también mantiene la orientación correcta cuando te mueves, así como poder diferenciar qué tipo de movimiento estás realizando.

El podómetro cuenta los pasos que da la persona que lleva el reloj. También hace uso del GPS para obtener información mucho más precisa. Ya

que va a poder medir la distancia recorrida, el tiempo que ha tardado y el número exacto de pasos que se han tenido que dar para recorrer la distancia en cuestión.

El GPS es un sistema de posicionamiento global que permite determinar la posición de alguien o algo en coordenadas precisas de latitud y longitud en cualquier punto del planeta en tiempo real. El receptor GPS recopila datos de diferentes satélites para calcular su posición como un conjunto de coordenadas. Esto le permite realizar un seguimiento de su ruta y la distancia.

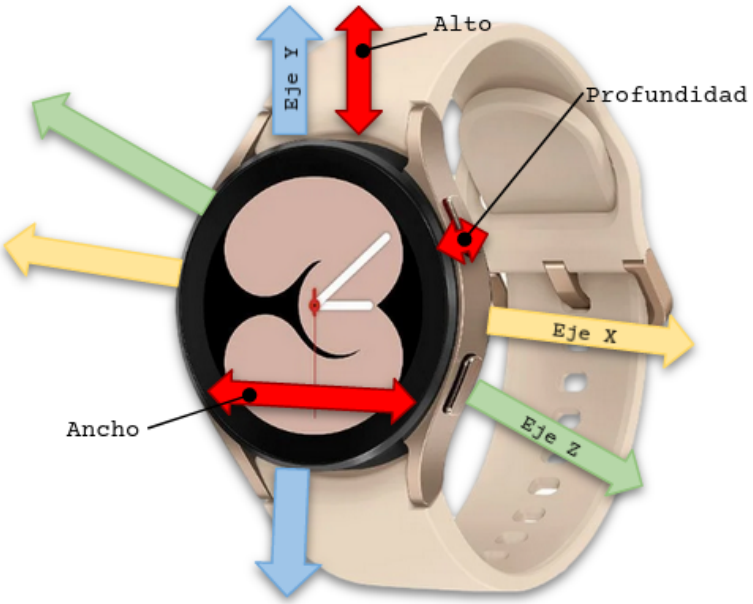

Figura 3.2.1. Acelerómetro

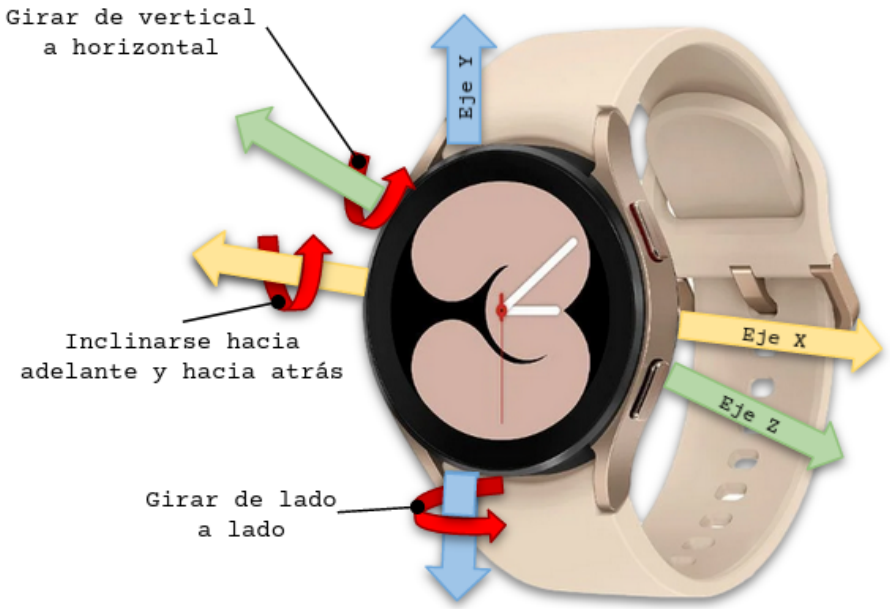

Figura 3.2.2. Giroscopio

Capítulo 4 Diseño de la aplicación y funcionalidades

En este apartado se define el objetivo, la idea y el diseño de la aplicación propuesta. Además, se describen las variables del sensor de la plataforma Android Developers para comprender cómo se recopilan los datos de las variables fisiológicas. Finalmente, se discute el análisis de los datos para determinar si la persona que conduce se está quedando dormida o no.

4.1 Objetivos

La Figura 4.1 muestra el diagrama de casos de uso de la aplicación, en el que se describe el proceso de extracción de datos de los sensores y variables del reloj inteligente. Luego, los datos se analizan para determinar si la persona que conduce muestra síntomas de somnolencia. Si esta no muestra síntomas de somnolencia y sigue conduciendo, se continúa con el monitoreo. Si no, se envía una alerta de vibración al reloj para despertarla. Finalmente, si quien conduce continúa conduciendo, las variables fisiológicas continúan siendo monitoreadas con los sensores.

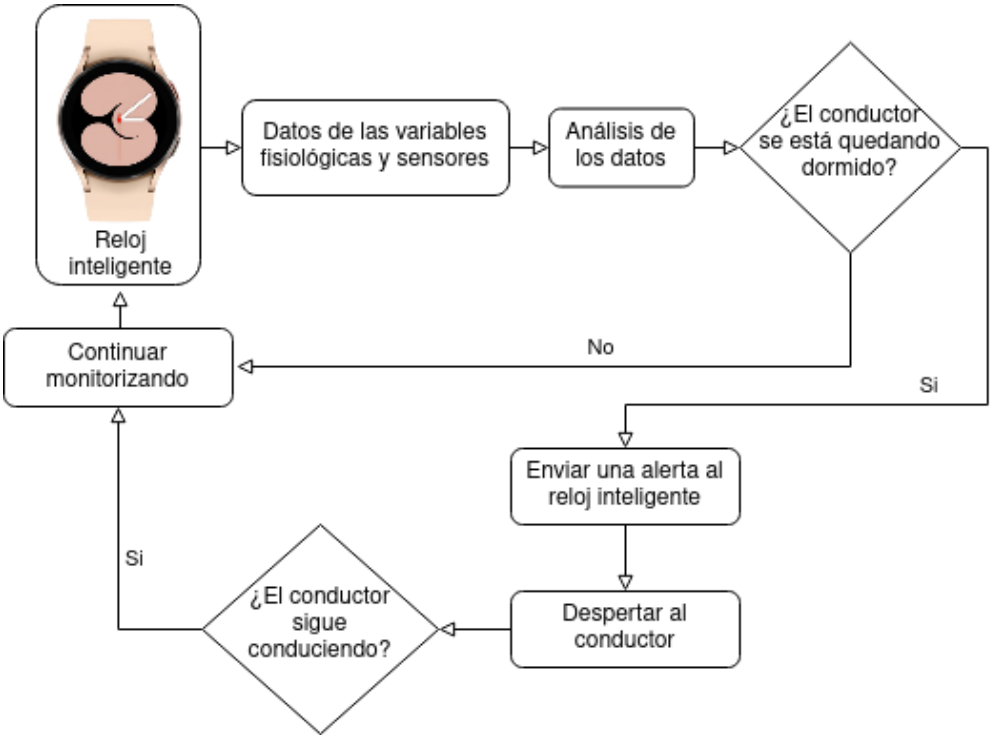

Figura 4.1. Diagrama de casos de uso de la aplicación

4.2 Datos de los sensores

La plataforma Android Developers tiene una clase pública *Sensor* cuyo propósito es definir las variables del sensor para obtener los datos del reloj inteligente. Hay varios sensores que le permiten monitorear el movimiento de un dispositivo: los sensores vectoriales para rotación, gravedad, aceleración lineal, movimiento significativo, contador de pasos y detector de pasos están basados en hardware o software, y los sensores de acelerómetro y giroscopio están siempre basados en hardware.

Las variables de los sensores más importantes se dividen en paquetes para almacenar las clases. En el paquete *android.hardware* las variables más importantes son: tipo acelerómetro, tipo giroscopio, tipo frecuencia cardíaca, tipo latido cardíaco y tipo contador de pasos. Todas estas variables tienen dos tipos de datos: *string* o *int*. El paquete *android.location* tiene la clase *Location* para representar la ubicación geográfica. El paquete *android.os* contiene la clase *Vibrator* para producir la alarma en el reloj. Estos son algunos de los ejemplos de clases y variables utilizadas en este trabajo.

4.3 Análisis de los datos

Los datos se pueden analizar con algoritmos utilizando dos tipos de aprendizaje: supervisado y no supervisado. El aprendizaje supervisado comienza con un conjunto predefinido de datos etiquetados, de modo que el valor del atributo de destino es el atributo que intenta predecir. El atributo de destino para el conjunto de datos se conoce a mano. Por otro lado, el aprendizaje no supervisado parte de datos previamente no etiquetados. Este trabajo asume inicialmente que no hay un conocimiento previo de los datos de una persona, por lo que en este caso, se usa un algoritmo no supervisado. Además, se considera el caso de medir los datos de interés en estado de reposo para poder utilizar un algoritmo supervisado.

Capítulo 5 Seguridad de la aplicación

Al proteger la seguridad de la aplicación, se mejora la confianza de los usuarios en ella. Por lo tanto, en su desarrollo, se ha tratado de seguir buenas prácticas de seguridad en la implementación del software.

En primer lugar, se ha intentado que la comunicación sea segura, protegiendo los datos que intercambia la aplicación con otras aplicaciones y sitios web, mejorando la estabilidad de la comunicación. Esto se logra mediante el uso de intenciones implícitas y proveedores de contenido no exportado (mostrando un selector de aplicaciones, aplicando permisos basados en firmas y deshabilitando el acceso a los proveedores de contenido de la aplicación), solicitando credenciales antes de mostrar información confidencial (por PIN, contraseña, patrón o credencial biométrica, como el reconocimiento facial o la huella dactilar), aplicando medidas de seguridad de la red (con el tráfico TLS (TLS, Transport Layer Security), agregando una configuración de seguridad de la red y creando un administrador de confianza propietario) y usando cuidadosamente los objetos WebView (a través de canales de mensajes HTML (HTML, HyperText Markup Language)). En segundo lugar, se ha tenido cuidado para garantizar que las solicitudes de permisos sean adecuadas, usando intentos para diferir los permisos y compartiendo datos de forma segura entre aplicaciones. En tercer lugar, se ha prestado atención al almacenamiento de datos, guardando datos privados en el almacenamiento interno, almacenando solo datos no confidenciales en archivos de caché y utilizando *SharedPreferences* en modo privado. En cuarto lugar, los servicios y dependencias han sido monitoreados en busca de actualizaciones verificando el proveedor de seguridad de *Google Play Services* y actualizando todas las dependencias de la aplicación.

Además, el uso de *SafetyNet* proporciona un conjunto de servicios y API (API, Application Programming Interfaces) que ayudan a proteger la aplicación contra amenazas de seguridad, que incluyen manipulación de dispositivos, direcciones URL (URL, Uniform Resource Locator) incorrectas, aplicaciones potencialmente dañinas y usuarios falsos. Cuenta con el sistema *Android Keystore* que protege el material de claves del uso no autorizado. Esto evita la extracción de material clave de los procesos de la aplicación y del dispositivo Android en su conjunto para reducir el uso no autorizado de claves fuera del dispositivo. Además, permite que las aplicaciones especifiquen usos autorizados de sus claves y aplica estas restricciones fuera de los procesos de la aplicación para reducir el uso no autorizado de material clave en el dispositivo.

5.1 Gestión de claves

Se utilizan dos conceptos para la gestión de claves. Por un lado, se utiliza un conjunto de claves para cifrar archivos o datos de preferencias compartidas, que se almacenan en *SharedPreferences*. Por otro lado, se utiliza una clave maestra, que cifra todos los conjuntos de claves y se almacena mediante el sistema de almacenamiento de claves de Android. La biblioteca de seguridad también incluye dos clases para proporcionar datos más seguros en reposo. En primer lugar, la clase de archivo cifrado se utiliza para proporcionar operaciones seguras de lectura y escritura desde flujos de archivos mediante el cifrado autenticado con datos asociados (AEAD, Authenticated Encryption with Associated Data). En segundo lugar, la clase *EncryptedSharedPreferences* se utiliza para cifrar automáticamente claves y valores mediante una combinación de dos esquemas: primero, las claves se cifran mediante un algoritmo determinista y, a continuación, los valores se cifran con AES-256, (AES, Advanced Encryption Standard) GCM (GCM, Galois Counter Mode) de forma no determinista.

5.2 Algoritmos criptográficos

La plataforma permite elegir diferentes algoritmos para cada clase. Para el cifrado se recomienda AES en modo CBC (CBC, Cipher Block Chaining) o GCM con claves de 256 bits (como AES/GCM/NoPadding), para *MessageDigest* la familia SHA-2 (SHA, Secure Hash Algorithm), para Mac el HMAC (HMAC, Hash-based Message Authentication Code) de la familia SHA y para firma el SHA- 2 familias con ECDSA (ECDSA, Elliptic Curve Digital Secure Algorithm) (como SHA256withECDSA).

Se puede escoger la ejecución de diferentes operaciones criptográficas al leer o escribir un archivo, cifrar un mensaje, generar un resumen de mensaje y generar o verificar una firma digital. En concreto, hay multitud de algoritmos disponibles compatibles con Android como son: DH (DH, Diffie Hellman), DSA (DSA, Digital Signature Algorithm), AES, BLOWFISH, ChaCha20, DES (DES, Data Encryption Standard), 3DES, EC (EC, Elliptic Curve), GCM, PKCS12PBE (PKCS12PBE, Public Key Cryptography Standards Password Based Encryption), X.509 (Public Key Infrastructure), ECDH (ECDH, Elliptic Curve Diffie Hellman), MD5 (Message Digest Algorithm 5), la familia SHA. Además, los algoritmos de encriptación AES, AES128, AES256, ARC4 (ARC4, Alleged Rivest's Cipher), BLOWFISH, ChaCha20, DES, 3DES y RSA (RSA, Rivest, Shamir y Adleman) le permiten elegir entre diferentes modos (CBC, ECB (ECB, Electronic CodeBook), GCM), y si lo desea, también puede elegir entre diferentes rellenos para el algoritmo elegido.

Capítulo 6 Conclusiones y líneas futuras

En este trabajo se ha diseñado una aplicación que recoge, a través de los sensores de un reloj inteligente, varios parámetros de algunas de las variables fisiológicas más relevantes que permiten detectar de forma precoz si una persona se está quedando dormida mientras conduce. En ese caso, la aplicación genera una alerta que despierta a la persona que conduce para evitar posibles accidentes en la carretera. Además, la implementación ha seguido las buenas prácticas recomendadas de programación de código seguro para proteger los datos sensibles que maneja la aplicación.

Actualmente se está estudiando la posibilidad de utilizar el sensor BIA con el fin de utilizar la impedancia para detectar el estado del tono muscular, así como los cambios en el tono muscular, ya que el tono muscular disminuye cuando una persona se está quedando dormida. Otra posible mejora es el uso del sensor de giroscopio para tratar de detectar el movimiento de caída de la muñeca en el coche debido a la somnolencia. Asimismo, para poder adaptar las alertas a todo tipo de personas, se definirán dos alarmas diferentes: la vibración del reloj y un estímulo sensorial auditivo con sonido.

Capítulo 7 Summary and conclusions

In this work, an application has been designed that collects, through the sensors of a smartwatch, several parameters of some of the most relevant physiological variables that allow early detection if a person is falling asleep while driving. In that case, the application generates an alert that wakes up the driver to avoid possible road accidents. In addition, the implementation has followed the recommended good practices of secure code programming to protect the sensitive data handled by the application.

The possibility of using the BIA sensor is currently being studied in order to use impedance to detect the state of muscle tone, as well as changes in muscle tone, since muscle tone decreases when a person is falling asleep. Another possible improvement is the use of the gyroscope sensor to try to detect the wrist dropping motion in the car due to drowsiness. Also, in order to adapt the alerts to all types of people, two different alarms will be defined: the vibration of the watch and an auditory sensory stimulus with sound.

Bibliografía

[1] Dirección General de Tráfico:"Conducir con sueño o cansancio", 2022. https://www.dgt.es/muevete-con-seguridad/evita-conductas-de-riesgo/Conducir-con-sueno-o-cansancio.

[2] Navarrete, R.I., Aguirre (2013), M.S.: "Cambios Fisiológicos en el Sueño", en Revista Ecuatoriana de Neurología, 22(1-3). https://cutt.ly/uWhhnwe.

[3] Becerril L., Jhaquelin E., Velázquez J. et al., Adolfo (2021, noviembre-diciembre), C.: "Una red neuronal para la detección de somnolencia en conductores", en Revista Digital Universitaria (rdu), 22(6). doi:http://doi.org/10.22201/cuaieed.16076079e. 2021.22.6.1.

[4] Vicente, J., Laguna, P., Bartra, A. et al.: "Drowsiness detection using heart rate variability", en Med Biol Eng Comput, 54, 927–937 (2016). doi:https://doi.org/10. 1007/s11517-015-1448-7.

[5] B. Lee, B. Lee and W. Chung: "Wristband-Type Driver Vigilance Monitoring System Using Smartwatch", en IEEE Sensors Journal, vol. 15, no. 10, pp. 5624-5633,Oct. 2015. doi:10.1109/JSEN.2015.2447012.

[6] G. Li, B. L. Lee and W. Y. Chung: "Smartwatch-Based Wearable EEG System for Driver Drowsiness Detection", en IEEE Sensors Journal, vol. 15, no. 12, pp. 7169-7180, Dec. 2015. doi:10.1109/JSEN.2015.2473679.

[7] M. Ramzan, H. U. Khan, S. M. Awan, A. Ismail, M. Ilyas and A. Mahmood: "A Survey on State-of-the-Art Drowsiness Detection Techniques", en IEEE Access, vol. 7, pp. 61904-61919, 2019. doi:10.1109/ACCESS.2019.2914373.

[8] P. Dewi Purnamasari and A. Zul Hazmi: "Heart Beat Based Drowsiness Detection System for Driver", en International Seminar on Application for Technology of Information and Communication, pp. 585-590, 2018. doi:10.1109/ISEMANTIC. 2018.8549786.

[9] S. Tateno, X. Guan, R. Cao and Z. Qu: "Development of Drowsiness Detection System Based on Respiration Changes Using Heart Rate Monitoring", en 57th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE), pp. 1664-1669, 2018. doi:10.23919/SICE.2018.8492599.

[10] Jo, S. H., Kim, J. M., Kim, D. K.: "Heart Rate Change While Drowsy Driving", en Journal of Korean medical science, 34(8), e56, 2019. doi:https://doi.org/10.3346/jkms.2019.34.e56.

[11] K. Fujiwara et al.: "Heart Rate Variability-Based Driver Drowsiness Detection and Its Validation With EEG", en IEEE Transactions on Biomedical Engineering, vol. 66, no. 6, pp. 1769-1778, June 2019. doi:10.1109/TBME.2018.2879346.

[12] Vicente J, Laguna P, Bartra A, Bailón R.: "Drowsiness detection using heart rate variability", en Med Biol Eng Comput., 2016 Jun;54(6):927-37. Epub 2016 Jan 16. PMID: 26780463. doi:10.1007/s11517-015-1448-7.

[13] Buendia R, Forcolin F, Karlsson J. et al: ”Deriving heart rate variability indices from cardiac monitoring-An indicator of driver sleepiness”. 2019;20(3):249-254. PMID: 30978124.doi:10.1080/15389588.2018.1548766.

[14] Awais M, Badruddin N, Drieberg M: ”A Hybrid Approach to Detect Driver Drowsiness Utilizing Physiological Signals to Improve System Performance and Wearability. Sensors (Basel)”. 2017 Aug 31;17(9):1991. doi:10.3390/s17091991.

Anexos

Anexo 1. Artículos enviados a congresos

Drowsiness detection in drivers with a smartwatch
Sonia Díaz-Santos, Pino Caballero-Gil
Workshop on Cybersecurity Applications and Intelligent Transportation Systems CAITS
Proceedings of the International Conference on Security and Management SAM
World Congress in Computer Science, Computer Engineering, and Applied Computing CSCE
Las Vegas, USA. July 25-28, 2022
Springer Nature
Indexada en Computing Research and Education (CORE), con ranking C
Indexada en CS Conference Rankings (0.83)
Indexada en GII-GRIN en Class WiP

Detección de somnolencia en conductores con un reloj inteligente
Sonia Díaz-Santos, Pino Caballero-Gil
XVII Reunión Española sobre Criptología y Seguridad de la Información RECSI.
Santander, 19-21 octubre 2022