(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 812 850**

(51) Int. CI.:

H04M 1/00	(2006.01)	*G01S 5/00*	(2006.01)
H04M 3/00	(2006.01)	*H04W 92/02*	(2009.01)
H04M 3/42	(2006.01)		
H04M 11/10	(2006.01)		
H04B 1/38	(2015.01)		
H04L 29/08	(2006.01)		
H04M 1/725	(2006.01)		
H04W 4/02	(2008.01)		
H04L 29/06	(2006.01)		
H04M 3/493	(2006.01)		

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.05.2002 E 16173420 (7)**

(97) Fecha y número de publicación de la concesión europea: **24.06.2020 EP 3082324**

(54) Título: **Servicios sensibles al contexto**

(30) Prioridad:

15.05.2001 US 854628

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.03.2021

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karakaari 7
02610 Espoo, FI

(72) Inventor/es:

NYKÄNEN, PETRI;
PALONIEMI, JARI y
KANGAS, PETRI

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Servicios sensibles al contexto

Antecedentes de la invención

Campo de la invención:

La invención descrita se refiere en general a métodos para proporcionar servicios de Internet y más particularmente se refiere a mejoras en el acceso de dispositivos móviles a servicios de Internet.

Técnica anterior:

Los teléfonos móviles y los asistentes digitales personales inalámbricos (PDA) pueden acceder a Internet mediante el Protocolo de aplicación inalámbrica (WAP). Los dispositivos inalámbricos habilitados para WAP ahora pueden acceder a aplicaciones de Internet como titulares de noticias, tasas de cambio, resultados deportivos, cotizaciones de bolsa, pronósticos del tiempo, diccionarios de frases multilingües, calendarios personales en línea, viajes en línea y servicios bancarios, o descargar tonos de llamada distintivos. Las redes inalámbricas de banda ancha hacen posible que los dispositivos inalámbricos habilitados para WAP intercambien mensajes multimedia que combinan texto convencional con tipos de contenido mucho más ricos, como fotografías, imágenes, clips de voz y videoclips. Los dispositivos inalámbricos habilitados para WAP se pueden usar para pagar facturas en línea usando el dispositivo inalámbrico como una billetera virtual. Los dispositivos inalámbricos habilitados para WAP pueden ofrecer servicios de transacciones y publicidad útiles e informativos de comerciantes en línea. Los dispositivos inalámbricos habilitados para WAP ahora también brindan servicios de entretenimiento, como juegos de aventura interactivos, concursos y torneos de ajedrez.

Lo que se necesita es la capacidad de un teléfono móvil o PDA inalámbrico para usar técnicas de inferencia de contexto para detectar el entorno del usuario móvil y, en respuesta, proporcionar información útil para el usuario que sea apropiada para el entorno percibido del usuario. Sería aún más útil descargar parte de la computación computacionalmente intensiva necesaria en las técnicas de inferencia de contexto, desde el dispositivo inalámbrico del usuario móvil a un servidor y a sitios web en Internet. Sería beneficioso mantener un perfil personal de las preferencias personales del usuario móvil en un servidor o sitio web en línea. Sería importante proporcionar al usuario móvil la capacidad de controlar cualquier acceso al perfil del usuario por el servidor en línea o el sitio web.

Datong Chen, Albrecht Schmidt, Hans-Werner Gellersen: "An Architecture for Multi-Sensor Fusion in Mobile Environments", actas de la 35ª Conferencia Internacional Annaul Hawaii, el 7 de enero de 2001, es un documento que analiza una arquitectura en capas para la fusión de múltiples sensores, aplicada para el reconocimiento ambiental de los dispositivos móviles personales. Este documento discute que el entorno de trabajo de los dispositivos móviles personales cambia dinámicamente dependiendo de las actividades de sus usuarios. Equipados con sensores, los dispositivos móviles pueden obtener un reconocimiento de su entorno de trabajo móvil, para mejorar su rendimiento con respecto a la usabilidad. La movilidad de los dispositivos presenta dos problemas para construir un sistema de reconocimiento. Primero, los contextos que debe cubrir un sistema de reconocimiento dependen de los usuarios, sus tareas y actividades, y también de los datos que se pueden obtener de diferentes sensores. En segundo lugar, el consumo de energía y el tamaño del dispositivo móvil limitan la capacidad de procesamiento de un sistema de reconocimiento. El documento presenta un diseño de un sistema de fusión basado en sensores de bajo costo, que puede ser reconfigurado por el usuario, para permitir un reconocimiento individualizado de los entornos. La arquitectura de software presentada en el documento está diseñada con cuatro capas diferentes, que pueden admitir reconfiguraciones en entornos móviles.

El documento US 6.073.075 describe un terminal móvil, y un método y sistema de suministro de información que proporciona inmediatamente información, que el usuario del terminal móvil desea, para el terminal móvil. Las áreas y la información de servicio relacionada se almacenan en la relación correspondiente en una base de datos. Un servidor de información que incluye medios para calcular el área de un destino del terminal móvil carga información sobre el área de destino desde la base de datos al terminal móvil que se mueve hacia el área de destino, utilizando medios de comunicación por radio antes de que el terminal móvil llegue al área de destino.

Sumario de la invención:

La invención se expone en las reivindicaciones independientes.

Ciertos ejemplos de la presente divulgación buscan proporcionar una invención de servicios web sensibles al contexto que permite a un teléfono móvil o PDA inalámbrico usar técnicas de inferencia de contexto para detectar el entorno del usuario y, en respuesta, proporcionar información útil para el usuario que sea apropiada para el entorno percibido del usuario.

Según un aspecto de la divulgación, existe un método para permitir que un dispositivo inalámbrico proporcione a su

usuario información útil que sea apropiada para el entorno actual del dispositivo. El método incluye las etapas de recibir señales del sensor que caracterizan un entorno actual del dispositivo inalámbrico; procesar las señales del sensor con un motor de inferencia de contexto; generar un resultado de contexto actual del procesamiento por motor de inferencia de contexto; y proporcionar información útil al usuario en respuesta al resultado del contexto actual. El procesamiento de las señales del sensor con un motor de inferencia de contexto se realiza como instrucciones programadas ejecutadas dentro del dispositivo inalámbrico del usuario. En otro aspecto de la divulgación, el procesamiento de las señales del sensor con un motor de inferencia de contexto se realiza como instrucciones programadas ejecutadas dentro de un servidor de red separado en respuesta a las señales del dispositivo inalámbrico del usuario. El servidor puede acceder a los archivos desde un servidor web, para el reenvío selectivo al dispositivo inalámbrico del usuario. El servidor puede mantener un perfil personal del usuario.

Un aspecto adicional de la divulgación proporciona el control del usuario del acceso de los programas de aplicación a los datos privados del usuario. Esto también puede incluir proporcionar control de acceso de los usuarios mediante programas de aplicación a los datos privados del usuario en el servidor. Aún más, esto también puede incluir proporcionar control de acceso del usuario por los programas de aplicación en un servidor web, a los datos privados del usuario.

Otro aspecto de la divulgación es proporcionar el resultado del contexto actual a un programa de aplicación en respuesta al control del usuario y recibir la información útil del programa de aplicación. Ciertos ejemplos permiten al usuario otorgar permiso de acceso al programa de aplicación para acceder al resultado del contexto actual. Esto se puede realizar en el dispositivo inalámbrico del usuario o en el servidor de red. El servidor de red puede llevar a cabo el control de acceso mediante programas de aplicación en servidores web, en respuesta a un perfil de privacidad del usuario recibido del dispositivo inalámbrico del usuario.

Descripción de las figuras:

La figura 1 es un diagrama de red de la invención, que muestra una relación de ejemplo entre el dispositivo inalámbrico portátil habilitado con el Protocolo de Aplicación Inalámbrica (WAP) del usuario, la puerta de enlace del protocolo WAP a Internet, el servidor de red, la Descripción Universal, registro de Descubrimiento e Integración (UDDI) y una pluralidad de sitios web.
La figura 1A muestra el dispositivo inalámbrico del usuario con las ACTUALIZACIONES DE PRIVACIDAD: submenú del menú de Servicios sensibles al contexto, que permite al usuario ACTUALIZAR SU PERFIL DE PRIVACIDAD o ACTUALIZAR SUS DATOS PERSONALES.
La figura 1B muestra el dispositivo inalámbrico del usuario con las CARACTERÍSTICAS ACTUALIZADAS DE PRIVACIDAD: submenú del menú de Servicios sensibles al contexto, lo que permite al usuario AUTENTICAR UN PROGRAMA y REGISTRAR UN PROGRAMA. Las figuras
1C y 1D muestran el dispositivo inalámbrico del usuario con el submenú EJECUTAR UNA APLICACIÓN del menú de Servicios sensibles al contexto, lo que permite al usuario EJECUTAR UNA APLICACIÓN.
La figura 2 es un diagrama de bloques funcional del dispositivo inalámbrico 100, que muestra sus diversos componentes y programas.
La figura 2A es un diagrama de bloques funcional del dispositivo inalámbrico 100, el servidor 140 y el servidor web 160, y su interacción al intercambiar un vector de metadatos 138 y datos de control de privacidad 150.
La figura 3 es un diagrama de flujo de proceso de red de la interacción del dispositivo inalámbrico 100, el servidor de red 140 y el servidor web 160 cuando se lleva a cabo la determinación del contexto actual del dispositivo inalámbrico 100.
La figura 4 es un diagrama de bloques funcional del servidor de red 140, que muestra la memoria que almacena los programas de software de servicios de aplicaciones necesarios para realizar las operaciones de la invención.

ANÁLISIS DE LA REALIZACIÓN PREFERIDA:

La invención de servicios web sensibles al contexto permite que un teléfono móvil o PDA inalámbrico use técnicas de inferencia de contexto para detectar el entorno del usuario y, en respuesta, proporcionar información útil para el usuario que sea apropiada para el entorno percibido del usuario. La invención descarga parte de la computación computacionalmente intensiva necesaria en las técnicas de inferencia de contexto, desde el dispositivo inalámbrico del usuario móvil a un servidor y a sitios web en Internet. La invención de servicios web sensibles al contexto mantiene un perfil personal de las preferencias personales del usuario móvil en un servidor o sitio web en línea. El usuario móvil tiene la capacidad de controlar el acceso de los programas de aplicación en el dispositivo inalámbrico a los datos privados del usuario. La invención de servicios web sensibles al contexto proporciona al usuario móvil la capacidad de controlar cualquier acceso al perfil del usuario por el servidor en línea o el sitio web.

El dispositivo inalámbrico del usuario móvil está equipado con un motor de inferencia de contexto para proporcionar y conocer el contexto del usuario móvil para los programas de aplicación, incluidas las aplicaciones de terceros. Dado que la potencia de procesamiento y la capacidad de almacenamiento están limitadas en los dispositivos inalámbricos típicos, los requisitos de carga y almacenamiento computacionales del motor de inferencia de contexto se distribuyen a un servidor de inferencia de contexto capaz de procesar los datos de contexto. La invención permite al usuario móvil controlar qué programas de aplicación en el dispositivo inalámbrico tienen acceso a la información de contexto privado

del usuario. Un bloqueo de control de privacidad en el dispositivo inalámbrico otorga o revoca el acceso de los programas de aplicación a la información de contexto privada, en función de las preferencias del usuario móvil almacenadas en un perfil de privacidad. El mismo control de privacidad y perfil de privacidad se extiende al servidor de inferencia de contexto, permitiendo así la extensión del control de privacidad del usuario a cualquier servidor web conectado al servidor de inferencia de contexto. La invención permite así construir una infraestructura para aplicaciones y servicios sensibles al contexto dentro del dispositivo inalámbrico y el servidor, mientras proporciona al usuario móvil control sobre la información de contexto del usuario de privacidad.

La invención se aplica a teléfonos inalámbricos y asistentes digitales personales inalámbricos (PDA) que implementan el estándar del Protocolo de Aplicación Inalámbrica (WAP). La figura 1 es un diagrama de red de una realización de la invención, que muestra una relación de ejemplo entre el dispositivo inalámbrico portátil 100 habilitado para el Protocolo de Aplicación Inalámbrica (WAP) del usuario, una puerta de enlace de protocolo WAP 120 y el servidor 140. El dispositivo inalámbrico portátil 100 habilitado para WAP del usuario puede ser un teléfono móvil inalámbrico, buscapersonas, radio bidireccional, teléfono inteligente, comunicador personal o similar. El dispositivo inalámbrico portátil 100 habilitado para WAP del usuario accede a un pequeño archivo llamado cubierta que está compuesto de varias páginas más pequeñas llamadas tarjetas que son lo suficientemente pequeñas como para caber en el área de visualización del micronavegador 102 del dispositivo. El tamaño pequeño del micronavegador 102 y los tamaños de archivo pequeños acomodan las restricciones de memoria bajas del dispositivo inalámbrico portátil 100 y las restricciones de ancho de banda bajo de una red inalámbrica 116. Las tarjetas se escriben en el Lenguaje de Marcas Inalámbrico (WML), que está ideado específicamente para pequeñas pantallas y navegación de una mano sin un teclado. El lenguaje WML es escalable desde pantallas de texto de dos líneas en el micronavegador 102 de un teléfono celular, hasta grandes pantallas LCD que se encuentran en teléfonos inteligentes y comunicadores personales. Las tarjetas escritas en el lenguaje WML pueden incluir programas escritos en WMLScript, que es similar a JavaScript, pero exige un mínimo de memoria y potencia de CPU del dispositivo 100 porque no contiene muchas de las funciones innecesarias que se encuentran en otros lenguajes de secuencias de comandos.

El Nokia WAP Client Versión 2.0 es un producto de software que contiene los componentes necesarios para implementar el cliente WAP 108 en el dispositivo inalámbrico 100. Estos componentes incluyen un navegador de lenguaje de marcado inalámbrico (WML), motor WMLScript, subsistema push y pila de protocolo inalámbrico. El Nokia WAP Client es un producto de código fuente que puede portarse e integrarse en dispositivos inalámbricos como teléfonos móviles y PDA inalámbricos. Los programas de aplicación 106 almacenados en el dispositivo inalámbrico 100 interactúan con el Cliente WAP 108 para implementar varias aplicaciones de comunicaciones. Los detalles del Nokia WAP Client Versión 2.0 se pueden encontrar en el documento en línea: Nokia WAP Client Version 2.0, Product Overview, Nokia Internet Communications, 2000, www.nokia.com/corporate/wap.

El Cliente WAP 108 incluye la función de infraestructura de clave pública inalámbrica (PKI), que proporciona la infraestructura y los procedimientos necesarios para la autenticación y las firmas digitales para servidores y clientes móviles. PKI inalámbrico es un sistema basado en certificados que utiliza pares de claves públicas/privadas asociadas con cada parte involucrada en una transacción móvil. El módulo de identidad inalámbrico (WIM) es una característica de token de seguridad del cliente WAP 108, que incluye características de seguridad, como las claves públicas y privadas y los certificados de servicio, necesarios para la autenticación del usuario y las firmas digitales. Además, tiene la capacidad de realizar operaciones criptográficas para cifrar y descifrar mensajes.

El dispositivo inalámbrico 100 de la figura 1 también tiene una pluralidad de sensores para detectar las condiciones ambientales del usuario móvil. Los sensores que se muestran incluyen SENSOR DE POSICIONAMIENTO 122, SENSOR DE TOQUE 124, SENSOR DE AUDIO 125, SENSOR DE COMPÁS 126, SENSOR DE LUZ AMBIENTE 128, SENSOR DE TEMPERATURA AMBIENTE 132 y SENSOR DE ACELERACIÓN DE TRES EJES 134. El sensor de audio 125 puede ser un micrófono, por ejemplo, que puede detectar el habla o los sonidos ambientales. El sensor de posicionamiento puede ser, por ejemplo, un receptor GPS integrado en el dispositivo. El sensor de posicionamiento también puede ser, por ejemplo, un sensor de triangulación de radiobaliza que determina la ubicación del dispositivo inalámbrico mediante una red de radiobalizas, estaciones base o puntos de acceso, como se describe, por ejemplo, en la patente europea EP de Nokia 0 767 594 A2, titulada "Mobile Station Positioning System". Estos sensores proporcionan entradas que son muestreadas por el dispositivo inalámbrico 100 para inferir un contexto actual, como se describirá a continuación.

La puerta de enlace de protocolo WAP 120 conecta Internet 130 y la red inalámbrica 116. La puerta de enlace de protocolo WAP 120 incluye la característica de infraestructura de clave pública inalámbrica (PKI) para ayudar a proporcionar una conexión segura de Internet al dispositivo inalámbrico 100. La puerta de enlace de protocolo WAP 120 permite que el dispositivo inalámbrico habilitado para WAP 100 acceda a aplicaciones de Internet como titulares de noticias, tipos de cambio, resultados deportivos, cotizaciones de acciones, viajes en línea y servicios bancarios, o descargar tonos de llamada distintivos.

El dispositivo inalámbrico portátil 100 habilitado para WAP del usuario se comunica con la torre de radio 114 y puede intercambiar mensajes para distancias de hasta varios kilómetros. Los tipos de redes inalámbricas 116 admitidas por el estándar WAP incluyen datos de paquetes digitales celulares (CDPD), acceso múltiple por división de código (CDMA), sistema global para comunicaciones móviles (GSM), acceso múltiple por división de tiempo (TDMA), GPRS,

Banda ancha 3G y similares.

El proceso general de comunicación entre el dispositivo inalámbrico habilitado para WAP del usuario (el cliente) 100, a través de la puerta de enlace de protocolo WAP 120, hasta el servidor 140 se asemeja a la forma en que las páginas web se sirven en Internet utilizando el Protocolo de transferencia de hipertexto (HTTP) o Protocolo World Wide Web:

[1] El usuario presiona una tecla de teléfono en el dispositivo 100 del usuario relacionada con el Localizador de Recursos Uniforme (URL) del servidor 140.
[2] El dispositivo 100 del usuario envía la URL, a través de la torre de radio 114 y la red inalámbrica 116, a la puerta de enlace 120 usando protocolos WAP.
[3] La puerta de enlace 120 traduce la solicitud WAP en una solicitud HTTP y la envía a través de Internet 130 al servidor 140, a través de las interfaces de Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP).
[4] El servidor 140 maneja la solicitud como cualquier otra solicitud HTTP recibida a través de Internet. El servidor 140 devuelve una plataforma WML o una página de Lenguaje de marcado de hipertexto (HTML) de vuelta a la puerta de enlace 120 utilizando programas de servidor estándar escritos, por ejemplo en programas de Interfaz de puerta de enlace común (CGI), servlets de Java o similares.
[5] La puerta de enlace 120 recibe la respuesta del servidor 140 en nombre del dispositivo 100 del usuario. Si la respuesta es una página HTML, se transcodifica a WML si es necesario. Luego, la codificación WML y WMLScript se codifica en un código de bytes que luego se envía al dispositivo 100 del usuario.
[6] El dispositivo del usuario 100 recibe la respuesta en el código de byte WML y muestra la primera tarjeta en el mazo en el micronavegador 102 al usuario.

En la figura 1, la puerta de enlace de protocolo 120 incluye una pila de protocolo WAP organizada en cinco capas diferentes. Una capa de aplicación es el entorno de aplicaciones inalámbricas, que ejecuta aplicaciones y servicios portátiles. Una capa de sesión es el protocolo de sesión inalámbrico, que proporciona métodos para el intercambio organizado de contenido entre aplicaciones cliente/servidor. Una capa de transacción es el protocolo de transacción inalámbrico, que proporciona métodos para realizar transacciones confiables. Una capa de seguridad es la seguridad de la capa de transporte inalámbrico, que proporciona autenticación, privacidad y conexiones seguras entre aplicaciones. La capa de transporte es el protocolo de datagrama inalámbrico, que protege las capas superiores de los requisitos únicos de los diversos protocolos de red inalámbrica, como CDPD, CDMA, GSM, etc. Puede encontrar información adicional sobre el estándar WAP y la pila de protocolos WAP en el libro de Charles Arehart, et al. titulado "Professional WAP", publicado por Wrox Press Ltd., 2000 (ISBN 1-861004-04-1).

En la figura 1, el dispositivo inalámbrico portátil del usuario 100 incluye el micronavegador 102 que muestra el menú de Servicios sensibles al contexto, para permitir al usuario navegar a través de las tarjetas que se muestran y seleccionar las opciones que están programadas por los programas de aplicación 106. El dispositivo 100 del usuario también incluye el programa cliente WAP 108 que se ha discutido previamente.

El menú de servicios sensibles al contexto visualizado por el micronavegador 102 en la figura 1 lo representa el programa cliente WAP 108 bajo el control de los programas de aplicación 106, que se muestran en las figuras 2 y 2A. El usuario puede seleccionar el tipo de sesión con el menú de Servicios sensibles al contexto, ya sea [A] ACTUALIZAR CARACTERÍSTICAS DE PRIVACIDAD o [B] EJECUTAR UNA APLICACIÓN. Si el usuario selecciona el tipo de sesión ACTUALIZAR CARACTERÍSTICAS DE PRIVACIDAD, el menú de Servicios sensibles al contexto de la figura 1 presenta al usuario el submenú ACTUALIZAR CARACTERÍSTICAS DE PRIVACIDAD desde el cual el usuario puede seleccionar las siguientes opciones:

[A] ACTUALIZAR LAS CARACTERÍSTICAS DE PRIVACIDAD:

[1] ACTUALIZAR TU PERFIL DE PRIVACIDAD
[2] ACTUALIZAR TUS DATOS PERSONALES
[3] AUTENTICAR UN PROGRAMA

La opción [1] de ACTUALIZAR SU PERFIL DE PRIVACIDAD lleva a un segundo submenú que se muestra en la figura 1A, que tiene las siguientes opciones:

[1] ACTUALIZAR TU PERFIL DE PRIVACIDAD

[a] Agregar un programa local a la lista de permisos
[b] Eliminar un programa local de la lista
[c] Agregar un programa de servidor a la lista de permisos
[d] Eliminar un programa de servidor de la lista
[e] Agregar un programa de red a la lista de permisos
[f] Eliminar un programa de red de la lista.

La opción [2] de ACTUALIZAR SUS DATOS PERSONALES conduce a otro submenú que se muestra en la figura 1A, que tiene las siguientes opciones:

[2] ACTUALIZAR TUS DATOS PERSONALES

[a] Actualizar la base de datos del servidor
[b] Actualizar la base de datos de la red.

La opción [3] de AUTENTICAR UN PROGRAMA, lleva a otro submenú que se muestra en la figura 1B, que tiene las siguientes opciones:
[3] AUTENTICAR UN PROGRAMA

[a] Solicitar el certificado de clave pública del programa
[b] Verificar firmas de certificados
[c] Verificar tiempo de validez
[d] Verificar el estado de revocación
[e] Comprobar si la autoridad de certificación en la lista de confianza
[f] Marcar el programa como autenticado.

La opción AUTENTICAR UN PROGRAMA llama al control de privacidad 150 del dispositivo inalámbrico 100 en la figura 2. Si un programa de aplicación A, B, X o Y ha sido verificado por una autoridad confiable para verificar su aceptabilidad, entonces la autoridad confiable habrá emitido un certificado digital en un código de autenticación de mensaje (MAC) que ha calculado para el programa de aplicación, que puede ser verificado por el control de privacidad 150. Mientras el control de privacidad 150 confíe en la autoridad confiable que emite el certificado digital, la autenticación del programa de aplicación es sencilla.
Una vez que el usuario móvil haya verificado el certificado digital del programa y esté satisfecho de que el programa de aplicación no subvertirá la integridad o seguridad de los datos privados del usuario, el usuario puede registrar el programa. El registro es la concesión por parte del usuario de permiso de acceso al programa, para acceder al contexto actual del dispositivo inalámbrico del usuario y/o para acceder a otras partes de los datos privados del usuario. Hay varios niveles de permiso que el usuario puede otorgar en dos categorías, [a] cuándo pueden tener lugar los accesos y [b] a qué datos se puede acceder.
La opción [4] de REGISTRAR UN PROGRAMA lleva a otro submenú que se muestra en la figura 1B, que tiene las siguientes opciones:
[4] REGISTRAR UN PROGRAMA

[a] Cuándo pueden tener lugar los accesos
[b] A qué datos se puede acceder

Para la primera categoría de [a] cuándo pueden tener lugar los accesos, el nivel más alto de permiso en esta categoría es que el acceso puede ocurrir en cualquier momento y sin previo aviso. El nivel más bajo de permiso en esta categoría es que el acceso solo puede ocurrir en momentos específicos o bajo condiciones específicas, y solo después de la notificación al usuario y la autorización específica del usuario. Para la segunda categoría de [b] a qué datos se puede acceder, el nivel más alto de permiso en esta categoría es acceder a conjuntos de datos ilimitados en los datos privados del usuario, incluida la información de contexto actual, los datos personales ingresados por el usuario, el historial de uso de Internet del usuario datos, los datos de cookies de Internet del usuario y los datos de uso del programa de aplicación del usuario. El nivel más bajo de permiso en esta categoría es que el acceso a cualquier información solo puede ocurrir después de la notificación al usuario y la autorización específica del usuario. El usuario puede configurar cualquier nivel de permiso entre el más alto y el más bajo y hacer que sea la base para el registro. El usuario puede incluir los términos de registro en un certificado digital firmado por el usuario y adjuntado al programa de aplicación. El certificado de registro puede ser presentado por el programa al control de privacidad 150 antes de un evento de acceso propuesto, el control de privacidad 150 para verificar automáticamente el estado de registro del programa. El certificado de registro se puede construir como sigue.

El control de privacidad 150 puede calcular un código de autenticación de mensaje (MAC) y su propia firma digital y agregarlo como un certificado a un programa de aplicación aceptable A, B, X o Y. El control de privacidad 150 puede incluir los términos de registro en el certificado digital. Luego, cuando el programa solicita acceso a los datos privados del usuario, el control de privacidad 150 puede verificar automáticamente el MAC y su propia firma digital para verificar que el programa no haya cambiado y el control de privacidad 150 también puede verificar automáticamente el estado de registro del programa. Esto se logra mediante el control de privacidad 150 que calcula un valor hash para todo el programa de aplicación A, B, X o Y (o una parte de él) y los términos de registro, y luego forma un código de autenticación de mensaje (MAC) desde valor hash. El control de privacidad 150 luego usa su clave privada PKI para firmar digitalmente el código de autenticación de mensaje (MAC). Los términos del registro, el MAC y la firma digital del control de privacidad se adjuntan al programa de aplicación A, B, X o Y como un certificado de registro.

Entonces, cada vez que el programa de aplicación A, B, X o Y solicite acceso a los datos de contexto del usuario o datos privados, el control de privacidad 150 requerirá que el programa de aplicación presente el certificado de registro para que el control de privacidad 150 pueda verificar que MAC se compara con un MAC calculado y que la firma digital presentada es genuina. El control de privacidad 150 puede conceder automáticamente permiso de acceso al programa

de aplicación, de acuerdo con los términos del registro.

Los métodos para generar y evaluar los códigos de autenticación de mensajes para asegurar la integridad de los datos se describen en el libro de Stephen Thomas titulado "SSL y TLS", publicado por John Wiley and Sons, 2000. Dos ejemplos de algoritmos para la autenticación de mensajes son el resumen de mensajes de RSA (MD5) y el algoritmo de hash seguro (SHA), ambos descritos en el libro de Stephen Thomas. Otra referencia que entra en mayor detalle en su discusión sobre los métodos de integridad de datos es el libro de Bruce Schneier titulado "Applied Cryptography - 2nd Edition" publicado por John Wiley and Sons, 1996. Los métodos para generar y evaluar firmas digitales para asegurar la fuente del programa digital se describen en el libro de Richard E. Smith titulado "Internet Cryptography", publicado por Addison Wesley, 1997.

Lo que se ha descrito aquí para el control de privacidad 150 en el dispositivo inalámbrico 100, es igualmente aplicable al control de privacidad 164 en el servidor de red 140 de la figura 2A. El control de privacidad 164 en el servidor de red 140 puede calcular el código de autenticación de mensaje (MAC) y su propia firma digital y agregarlo, con los términos del registro, como un certificado de registro a un programa de aplicación aceptable en el servidor web 160. El control de privacidad 164 tiene una copia en caché 144 del Perfil de privacidad 152 del dispositivo inalámbrico 100. Esto permite procesar automáticamente la verificación de privacidad en el servidor de red 140 para las solicitudes de acceso del servidor web 160. Cuando el programa de aplicación en el servidor web 160 solicita acceso a los datos privados del usuario en el servidor de red 140 o en el dispositivo inalámbrico 100, el control de privacidad 164 en el servidor de red 140 requerirá que el programa de aplicación en el servidor web 160 presente el certificado de registro para que pueda verificar el MAC y su propia firma digital para verificar que el programa de la aplicación no haya cambiado. El control de privacidad 164 puede conceder automáticamente permiso de acceso al programa de aplicación en el servidor web 160, de acuerdo con los términos del registro.

Si el usuario selecciona el tipo de sesión [B] EJECUTAR UNA APLICACIÓN, el menú de Servicios sensibles al contexto de la figura 1C presenta al usuario el submenú EJECUTAR UNA APLICACIÓN desde el cual el usuario puede seleccionar las siguientes opciones:

[1] MENSAJERÍA

[a] intercambiar mensajes multimedia

[2] COMERCIO MÓVIL

[a] calendario personal en línea
[b] tipos de cambio
[c] servicios bancarios
[d] pagar facturas en línea usando billetera virtual
[e] publicidad útil e informativa
[f] servicios de transacciones comerciales en línea

El menú de Servicios sensibles al contexto de la figura 1D presenta al usuario el submenú EJECUTAR UNA APLICACIÓN del cual el usuario puede seleccionar las siguientes opciones:
[3] ENTRETENIMIENTO

[a] noticia titular
[b] resultados deportivos
[c] cotizaciones de acciones
[d] pronósticos del tiempo
[e] diccionarios de frases multilingües
[f] viajes en línea
[g] descarga de tonos de llamada distintivos
[h] juegos interactivos

La opción EJECUTAR UNA APLICACIÓN llama a uno de los programas de aplicación A, B, X o Y del dispositivo inalámbrico 100 en la figura 2.

La figura 2 es un diagrama de bloques funcional del dispositivo inalámbrico 100, que muestra sus diversos componentes y programas. El dispositivo inalámbrico 100 tiene aplicaciones contextuales A, B, X e Y, descargadas o en firmware. El dispositivo inalámbrico 100 no necesita utilizar una funcionalidad externa en la red para el muestreo inicial y la digitalización de las entradas del sensor. Los valores muestreados y digitalizados de las entradas del sensor son METADATA DE POSICIONAMIENTO 122', METADATA DE TOQUE 124', METADATA DE AUDIO 125', METADATA DE COMPÁS 126', METADATA DE LUZ AMBIENTE 128', METADATA DE TEMPERATURA AMBIENTE 132' y METADATA DE ACELERACIÓN DE TRES EJES 134'. Los valores muestreados y digitalizados de las entradas del sensor se cargan en un vector de metadatos 138.

La figura 2 muestra la memoria 202 del dispositivo inalámbrico 100, conectado por el bus 204 al teclado 104, la radio 206, la interfaz del sensor 208, el procesador central 210 y la pantalla 212. La memoria 202 almacena programas que son secuencias de instrucciones ejecutables que, cuando se ejecutan por el procesador 210, llevan a cabo los métodos de la invención. La memoria 202 almacena el programa cliente WAP 108, el motor de inferencia de contexto 136, el control de privacidad 150, el perfil de privacidad 152, la API de contexto 154, la API de movimiento/gesto 156, la API de ubicación 158 y otras API 162. El motor de inferencia de contexto 136 procesa el vector de metadatos 138 para producir el contexto actual. Los programas de aplicación 106 almacenados en la memoria 202 incluyen los programas de aplicación A y B que forman parte del sistema de software SS1, y los programas de aplicación X e Y que están contenidos en el entorno de ejecución "Ent. Ejec".

Si hay suficiente potencia computacional y capacidad de almacenamiento disponible en el dispositivo inalámbrico 100, puede tener lugar un procesamiento adicional del vector de metadatos 138 en el motor de inferencia de contexto 136, con el objetivo de producir el resultado de un contexto actual inferido. Sin embargo, si en algún momento del cálculo, el motor de inferencia de contexto 136 necesita la potencia de procesamiento o la capacidad de almacenamiento disponible en el servidor de red 140, el vector de metadatos 138 se envía desde el dispositivo inalámbrico 100 al motor de inferencia de contexto 142 en el servidor de red 140 de la figura 2A. El motor de inferencia de contexto 142 en el servidor de red 140 puede realizar el procesamiento requerido en el vector de metadatos 138 y luego devolverlo al motor de inferencia de contexto 136 en el dispositivo inalámbrico 100 para completar el resultado de contexto actual inferido. Alternativamente, el motor de inferencia de contexto 142 en el servidor de red 140 puede completar el procesamiento requerido y luego devolver el contexto actual inferido resultante al dispositivo inalámbrico 100.

La figura 2 muestra la arquitectura de un dispositivo inalámbrico con soporte para el reconocimiento del contexto. El reconocimiento del contexto se basa en la información sensorial recibida de varios tipos de sensores ubicados físicamente en el teléfono que se muestra en la figura 1. Los sensores que se muestran incluyen SENSOR DE POSICIONAMIENTO 122, SENSOR DE TOQUE 124, SENSOR DE AUDIO 125, SENSOR DE COMPÁS 126, SENSOR DE LUZ AMBIENTE 128, SENSOR DE TEMPERATURA AMBIENTE 132 y SENSOR DE ACELERACIÓN DE TRES EJES 134. Los sensores también se pueden ubicar en cubiertas de teléfonos similares a accesorios o en un accesorio inalámbrico como un dispositivo con Bluetooth. Los sensores también pueden ubicarse en el entorno, como en las habitaciones o vehículos del usuario. También se puede usar la duración del tiempo de uso de un teléfono y otra información disponible junto con los datos del sensor en los servicios de conocimiento de contexto.

La figura 2 muestra los datos del sensor recibidos de los sensores 122, 124, 125, 126, 128, 132 y 134 procesados por el Motor de Inferencia de Contexto 136. Los programas de aplicación A, B, X o Y que se ejecutan en el dispositivo inalámbrico 100, pueden proporcionar opcionalmente datos de aplicación al motor de inferencia de contexto 136, junto con su solicitud de contexto actual. El motor de inferencia de contexto 136 puede procesar opcionalmente las señales del sensor y los datos de la aplicación para producir el contexto actual. El motor de inferencia de contexto 136 luego alimenta el contexto actual a través de varias API 154, 156, 158 y 162 a los programas de aplicación A, B, X e Y. Los programas de aplicación pueden registrarse en la interfaz de programación de aplicaciones 154 para recibir el contexto actual o cambios en el contexto. Esto permite la sensibilidad al contexto en los programas de aplicación.

La figura 2 muestra los programas de aplicación "nativos" A y B que se ejecutan en un primer sistema de software SS1 del dispositivo inalámbrico 100. El término "Sistema de software" se utiliza aquí para cualquier entorno con capacidad de ejecución. Este primer sistema de software puede ser propietario o estar basado en un sistema operativo en tiempo real disponible comercialmente, como NOS, ISA, EPOC, JAVA o WAP. Los programas de aplicaciones de terceros X y se ejecutan dentro de un entorno de ejecución. Este entorno de ejecución puede limitar las capacidades del sistema disponibles para los programas de aplicación, como el acceso a las API (comportamiento fijo, no dinámico).

La figura 2 muestra la función de control de privacidad del usuario móvil. La característica de control de privacidad permite al usuario designar qué programas de aplicación tienen acceso a las API 154 de conocimiento de contexto para utilizar la información de contexto actual producida por el motor de inferencia de contexto 136. Todas las solicitudes o registros de los programas de aplicación A, B, X e Y para tener acceso al motor de inferencia de contexto 136, primero deben pasar por el bloque de Control de privacidad 150. El bloque de Control de privacidad 150 utiliza la verificación de datos de seguridad del usuario almacenada en el Perfil de privacidad 152 para otorgar derechos de acceso a los programas de aplicación solicitantes. El usuario controla la concesión de derechos de acceso por medio de la entrada de datos de seguridad del usuario a través de la interfaz de usuario. Los datos de seguridad del usuario incluyen la lista de permisos 155, los certificados 157 de Infraestructura de clave pública (PKI), la lista de confianza de la autoridad confiable de PKI 159 y las marcas establecidas por el usuario para aquellos programas de aplicación que han sido autenticados por los procedimientos de PKI, conjunto de datos 161. El usuario puede actualizar los datos de seguridad del usuario con el menú ACTUALIZAR CARACTERÍSTICAS DE PRIVACIDAD que muestra el dispositivo inalámbrico 100 que se muestra en las figuras 1A e IB. Se puede otorgar acceso a un programa de aplicación basado en su firma digital, que es parte de las aplicaciones del sistema u otros medios conocidos en la técnica. También es posible proporcionar una interfaz de usuario de privacidad independiente de todo el sistema para el control de privacidad 150, que puede ser utilizada por el usuario móvil para establecer las políticas de privacidad y alertar al usuario móvil de que un programa de aplicación está intentando registrarse para recibir el información de conocimiento del contexto privado del usuario. El control de privacidad 150 y el Perfil de privacidad 152 permiten al usuario móvil otorgar, denegar o revocar el acceso, otorgar acceso por un tiempo limitado o requerir que un programa de aplicación

solicite siempre el registro antes de que el usuario otorgue acceso.

En la figura 2, el motor de inferencia de contexto 136 en el dispositivo inalámbrico 100 hace inferencias de todas las entradas de sensor en función de dónde está ubicado el dispositivo inalámbrico por el usuario móvil. Por ejemplo, el contexto actual inferido del dispositivo 100 puede estar "EN EL BOLSILLO DEL USUARIO", cuando un cierto conjunto de sensores ingresa una combinación específica de señales que tienen un rango de valores específico. Como ejemplo, la inferencia resultante del contexto actual por el Motor de interferencia de contexto 136 podría expresarse en formato de lenguaje XML de la siguiente manera:

```
<Context Inference Engine in Device>
   <device placement> pocket </ device placement>
   <User Interface state> sleep mode </User Interface state>
   < device location> in elevator 5 building 1 floor 2</ device location>
   <API active actions> meeting starting on floor 3 room 322 </API active actions>
   </Context Inference Engine in Device >
```

El motor de inferencia de contexto 136 en el dispositivo inalámbrico 100 puede realizar el proceso de inferencia de contexto con cualquiera de varios métodos. Se puede ponderar información de entrada diferente de los sensores de acuerdo con su valor relativo de importancia apropiado para cada condición o situación del entorno a analizar. Cada sensor tiene su propio valor de peso. Alternativamente, los valores de peso para cada sensor para cada condición ambiental se pueden aprender de las sesiones de entrenamiento utilizando, por ejemplo, redes neuronales artificiales (ANN), mapas autoorganizados (SOM), árboles de decisión, sistemas difusos basados en reglas o modelos basados sistemas como el modelado oculto de Markov (HMM). Se pueden usar combinaciones de dos o más de los métodos alternativos, dependiendo de la aplicación.

El motor de inferencia de contexto 136 puede adaptar continuamente sus pesos a través de métodos de aprendizaje adaptativos y continuos, donde el usuario enseña al dispositivo inalámbrico 100 nuevas condiciones ambientales y las nombra. El modelado oculto de Markov (HMM) se puede utilizar, por ejemplo, para implementar un método de aprendizaje adaptativo y continuo para el motor de inferencia de contexto 136. Alternativamente, el dispositivo inalámbrico 100 puede programarse para reconocer espontáneamente una escena cambiada comparándola con escenas conocidas. El usuario puede enseñar al dispositivo inalámbrico nuevas condiciones ambientales y nombrarlas, utilizando la capacidad de aprendizaje adaptativo y automático de las redes neuronales. Los métodos de aprendizaje adaptativo y continuo son computacionalmente intensivos y son candidatos apropiados para colocar en el servidor de red 140, que ayuda al dispositivo inalámbrico 100, como se discute a continuación.

El campo de inferencia de contexto ha aplicado los principios del reconocimiento automatizado de patrones para procesar diversos tipos de entradas de sensores. El reconocimiento de voz se ha aplicado al procesamiento de señales de voz y el reconocimiento de escritura a mano se ha aplicado al procesamiento de señales de fuerza manual y acelerómetro. En el campo de la robótica, el reconocimiento de imágenes se ha aplicado al procesamiento de imágenes fijas y en movimiento digitalizadas, el reconocimiento de ubicación mecánica se ha aplicado al procesamiento de señales de láser y sonda de rango de sonda, y el reconocimiento de movimiento mecánico se ha aplicado al procesamiento de señales de inercia, aceleración y rumbo. En el campo de los dispositivos protésicos, el reconocimiento táctil se ha aplicado al procesamiento de señales de sensores táctiles. En el campo de la medicina, los programas de diagnóstico automatizados reconocen diversas patologías mediante el procesamiento de señales de campo bioeléctrico, así como las señales más tradicionales de pulso, frecuencia respiratoria y temperatura corporal. Estos diversos procesos de reconocimiento de señal del sensor tienen la característica común de que se lleva a cabo una etapa de entrenamiento inicial donde las señales muestreadas se equiparan con un modelo estadístico para esas señales.

Los principios del reconocimiento automatizado de patrones para estas diversas entradas de sensores se ejemplifican mediante las técnicas para reconocer patrones de voz. Una técnica común utilizada en el reconocimiento de voz es Modelado Oculto de Markov (HMM). El término "Oculto" se refiere a los eventos probabilísticos y no directamente observables que subyacen a una señal de voz. Los sistemas de reconocimiento de voz HMM suelen utilizar realizaciones de fonemas que son modelos estadísticos de segmentos fonéticos que tienen parámetros que se estiman a partir de un conjunto de ejemplos de entrenamiento. Los modelos de palabras se hacen encadenando o vinculando modelos estadísticos apropiados de segmentos fonéticos. Los modelos estadísticos sirven como estándares que deben coincidir con las señales de voz desconocidas que deben reconocerse.

El reconocimiento de señales de voz desconocidas requiere muestreo y digitalización de los fonemas hablados del hablante. Estos fonemas digitalizados se procesan en metadatos. Los metadatos se comparan con los modelos estadísticos estándar de fonemas. Las coincidencias más probables son el resultado del reconocimiento de voz inferido.

El reconocimiento consiste en encontrar la ruta más probable a través del conjunto de modelos de palabras para la señal de voz de entrada. Los sistemas de decodificación de reconocimiento de voz HMM primero deben ser entrenados a través de un proceso iterativo. El sistema debe estar expuesto a ejemplos de capacitación o palabras de la voz de un hablante en particular. Se analiza una palabra de entrenamiento para generar una secuencia enmarcada de

parámetros acústicos o modelos estadísticos. Un reconocimiento válido o "bueno" ocurre cuando la ruta más probable a través del conjunto de modelos de palabras para la palabra de entrenamiento resulta en reconocer la palabra de entrenamiento correcta.

Algunas referencias útiles que discuten los principios de los modelos ocultos de Markov son:

Rabiner, L.R., "A tutorial on hidden Markov models and selected applications in speech recognition", Actas del IEEE, volumen 77, número 2, 1989, páginas 257-286.
Rabiner, LR y Juang, BH, "An introduction to hidden Markov models", IEEE ASSP Magazine, enero de 1986, páginas 4-15.
Fraser, Andrew M. and Dimitriadis, Alexis, "Forecasting Probability Densities by Using Hidden Markov Models with Mixed States", Time Series Prediction: Forecasting the Future and Understanding the Past, Addison-Wesley, editor Weigend, Andreas S. y Gershenfeld, Neil A., 1994.
Charniak, Eugene, Statistical Language Learning, MIT Press, Cambridge, Massachusetts, 1993.

Para ilustrar cómo el Modelado Oculto de Markov (HMM) puede extenderse más allá del reconocimiento de voz, aquí se da un ejemplo para el reconocimiento táctil. En la etapa de entrenamiento para el reconocimiento táctil, las señales del sensor táctil se introducen al tocar un transductor táctil a una textura áspera, como por ejemplo papel de lija. Las señales del sensor táctil se transforman en un modelo estadístico de la señal de entrada. El modelo estadístico se almacena como estándar en la memoria de un ordenador bajo el identificador "textura_gruesa". Para ampliar el rango de señales del sensor que se incluyen en el modelo para "textura aproximada", se pueden realizar varias sesiones de entrenamiento, cada una con una dirección o presión diferente para tocar el papel de lija, lo que da como resultado varias muestras diferentes del modelo estadístico. El conjunto de muestras del modelo estadístico se almacena como estándar bajo el identificador "textura_gruesa". Otras sesiones de entrenamiento se llevan a cabo con una textura suave, como el vidrio. Las señales del sensor táctil que ingresan al tocar el transductor táctil con la textura suave se transforman en un modelo estadístico de la señal de entrada y se almacenan como un estándar bajo el identificador "textura_suave". Más tarde, en el modo de reconocimiento, un objeto desconocido es tocado por el transductor táctil, lo que resulta en una muestra de señal del sensor táctil. El reconocimiento de señales táctiles desconocidas requiere muestreo y digitalización de las señales del transductor táctil. Estas señales de sensor digitalizadas se procesan en metadatos. Los metadatos se comparan luego con los modelos estadísticos estándar de "textura_gruesa" y "textura_suave". La coincidencia más probable es el resultado del reconocimiento táctil inferido.

Las combinaciones de dos o más tipos de sensores pueden combinar sus señales en un vector de metadatos de entrada que caracteriza un evento de muestreo compuesto. El evento de muestreo compuesto puede reconocerse utilizando los principios del modelado oculto de Markov (HMM). Un ejemplo de evento de muestreo compuesto puede ser el estado de salud y fatiga del usuario de un dispositivo inalámbrico 100. Por ejemplo, un dispositivo inalámbrico 100 puede estar equipado con un transductor táctil que emite señales del sensor táctil en respuesta a la fuerza manual y la frecuencia del pulso del usuario que está agarrando el dispositivo inalámbrico 100. El dispositivo inalámbrico 100 puede estar equipado con un sensor de temperatura que emite señales de temperatura corporal en respuesta al usuario que agarra el dispositivo inalámbrico 100. El modelado oculto de Markov (HMM) se puede utilizar para reconocer un vector de metadatos de entrada de fuerza/temperatura que caracteriza la combinación de la fuerza manual y las señales del sensor de temperatura resultantes de un evento de muestreo. Un evento de muestreo compuesto en este ejemplo puede tener una duración extendida para que el sensor de fuerza pueda transducir la frecuencia del pulso del usuario durante un período de tiempo.

En la etapa de entrenamiento, las señales del sensor táctil y las señales del sensor de fuerza se emiten mientras el usuario está en buenas condiciones de salud y descansa normalmente. Las señales del sensor táctil y las señales del sensor de fuerza se combinan en un vector de metadatos de entrada de fuerza/temperatura que se transforma en un modelo estadístico de las señales de entrada. El modelo estadístico se almacena como un estándar en la memoria de la computadora del dispositivo inalámbrico 100 bajo el controlador "buena_salud_descansando_normalmente". Se realizan otras sesiones de entrenamiento con el usuario en diferentes estados de salud y fatiga. Por ejemplo, el usuario puede estar entrenando el dispositivo inalámbrico 100 mientras trabaja a altas horas de la noche en la oficina. Las señales del sensor táctil y las señales del sensor de fuerza resultantes de sostener el dispositivo inalámbrico 100, se combinan en un vector de metadatos de entrada de fuerza/temperatura para el usuario en condiciones de gozar de buena salud pero fatigado. El vector de metadatos de entrada de fuerza/temperatura se transforma en un modelo estadístico de las señales de entrada y se almacena como un estándar bajo el identificador "buena_salud_fatigado".

Más tarde, en el modo de reconocimiento, cuando el usuario sostiene el dispositivo inalámbrico 100, se muestrean las señales del sensor táctil y las señales del sensor de fuerza. El reconocimiento del Estado de Salud/Fatiga consiste en muestrear y digitalizar las señales del transductor táctil. Estas señales de sensor digitalizadas se procesan en un vector de metadatos. El vector de metadatos se compara con los modelos estadísticos estándar de manejo "buena_salud_descansando_normalmente" y "buena_salud_fatigado". La coincidencia más probable es el resultado del reconocimiento táctil inferido.

De acuerdo con la invención, este resultado de reconocimiento puede ser utilizado por un programa de aplicación de mantenimiento de salud en el dispositivo inalámbrico 100, para proporcionar información útil y apropiada al usuario.

Por ejemplo, un programa de mantenimiento de la salud puede procesar el resultado del reconocimiento y, en respuesta, enviar una señal de alarma al usuario y proporcionar sugerencias de medicamentos para paliar la fatiga detectada. Un problema con los programas de reconocimiento automático es que son relativamente grandes o llaman a bases de datos que son relativamente grandes en comparación con la capacidad de memoria del dispositivo inalámbrico 100.

Otro aspecto de la invención es que el resultado de reconocimiento puede ser utilizado por un programa de aplicación complementario en un servidor remoto, para proporcionar información adicional y más útil y apropiada para el usuario. Por ejemplo, el servidor puede acceder a una gran base de datos de sugerencias de medicamentos para paliar la fatiga detectada por el usuario. Los resultados de la búsqueda de la base de datos pueden devolverse al dispositivo inalámbrico 100. El servidor también puede mantener un perfil personal de las características y preferencias del usuario y puede usar ese perfil para formular automáticamente su consulta a la base de datos. Por ejemplo, las alergias a medicamentos del usuario pueden almacenarse en la base de datos del servidor, para asegurar que no se hagan recomendaciones que den como resultado una reacción alérgica del usuario al medicamento sugerido.

La figura 2A es un diagrama de bloques funcional del dispositivo inalámbrico 100, el servidor 140 y el servidor web 160, y su interacción al intercambiar el vector de metadatos 138 y los datos de control de privacidad 150'. Estos intercambios se encriptan en masa con una clave de sesión simétrica, como una clave de Estándar de cifrado de datos (DES), para proteger la privacidad de los datos. Para asegurar la integridad del vector de metadatos 138 y los datos de control de privacidad 150', se puede calcular y adjuntar un código de autenticación de mensaje (MAC) a los datos, como se describe en el libro referenciado anteriormente por Stephen Thomas titulado "SSL y TLS", publicado por John Wiley and Sons, 2000. Para asegurar que la fuente del vector de metadatos 138 y los datos de control de privacidad 150’ no puedan ser repudiados, se puede agregar una firma digital a los datos, como se describe en el libro de referencia de Richard E. Smith titulado "Internet Cryptography", publicado por Addison Wesley, 1997.

La figura 2A muestra el alcance de la implementación de conocimiento de contexto distribuido. El dispositivo inalámbrico 100 tiene aplicaciones sensibles al contexto A, B, X e Y descargadas o en firmware. El dispositivo inalámbrico 100 puede preprocesar localmente parte de la información de contexto en el vector de metadatos 138 antes de enviarlo al motor de inferencia de contexto 142 en el servidor de red 140 que es capaz de procesar los datos y responder de nuevo con el contexto actual resultante. El dispositivo inalámbrico 100 puede ejecutar programas de aplicación que requieren acceder al servidor de servicio web 160 para proporcionar servicios sensibles al contexto para el usuario móvil.

La figura 2A muestra cómo el procesamiento de los datos del sensor desde los sensores en el dispositivo inalámbrico 100 puede distribuirse entre el dispositivo inalámbrico y el servidor de red 140. La operación en la figura 2A es la siguiente:

1. Los sensores proporcionan continuamente los datos del sensor al motor de inferencia de contexto 136 en el dispositivo inalámbrico 100.
2. Un programa de aplicación que utiliza las API 154 de conocimiento de contexto puede solicitar la información de contexto más reciente, o el programa de aplicación puede registrarse para recibir cualquier cambio en la información de contexto específica.
3. El motor de inferencia de contexto 136 contacta de forma segura con el motor de inferencia de contexto 142 del servidor de red 140 y envía el vector de metadatos 138 al servidor 140. Dependiendo de los sensores y los detalles de implementación, Motor de inferencia de contexto 136 puede preprocesar parte de los datos del sensor en el vector de metadatos 138 antes de enviarlo. Dependiendo de los sensores y el intervalo de procesamiento, puede haber una conexión virtual abierta entre el Motor de inferencia de contexto 136 y el Motor de inferencia de contexto 142 para intercambios de datos frecuentes. El Motor de inferencia de contexto 142 en el servidor de red 140 tiene el poder de procesamiento y la capacidad de memoria para manejar el procesamiento computacionalmente intensivo y/o intensivo en memoria de los datos del sensor preprocesados en el vector de metadatos 138 para producir la información del resultado del contexto actual.
4. El Motor de inferencia de contexto 142 en el servidor de red 140 puede utilizar información de usuario local (información de historial, detalles del cliente) almacenada en la base de datos de usuario 146 para hacer una determinación más precisa del contexto actual del usuario móvil.
5. El motor de inferencia de contexto 142 en el servidor de red 140 luego devuelve de forma segura la información de conocimiento de contexto actual al motor de inferencia de contexto 136 en el dispositivo inalámbrico 100.
6. El motor de inferencia de contexto 136 en el dispositivo inalámbrico 100 proporciona entonces la información actual de conocimiento de contexto a través de las API de conocimiento de contexto 154 a los programas de aplicación registrados para recibir esa información.

La figura 2A muestra cómo los Servicios web en el Servidor de servicios web 160 están habilitados para recibir los resultados del contexto actual del dispositivo inalámbrico 100. El servidor de servicios web 160 tiene un sistema de software para el programa de aplicación de servidor A y un entorno de ejecución para los programas de aplicación de servidor X e Y que son similares al sistema de software SS1 y el entorno de ejecución (Ent. Ejec.) En el dispositivo inalámbrico 100 que se muestra en la figura 2. Los programas de aplicación de servidor A, X e Y en el servidor de servicio web 160 pueden requerir acceso a través de las API de conocimiento de contexto para proporcionar servicios

web con el contexto actual del dispositivo inalámbrico 100.

En la figura 2A, el Servidor de servicio web 160 usa el Cliente de inferencia de contexto 176 para contactar al Servidor de inferencia de contexto 174 en el servidor de red 140. El Cliente de inferencia de contexto 176 puede utilizar la información de la base de datos del cliente en la base de datos 184 para mejorar las capacidades de sensibilidad al contexto del servidor web 160. El contacto con el servidor de red 140 se realiza a través de una interfaz de conocimiento de contexto 186 al Servidor de inferencia de contexto 174 en el servidor de red 140.

El servidor de inferencia de contexto 174 registra los servicios web del servidor web 160 a través del control de privacidad 164 del servidor de red 140 en el motor de inferencia de contexto 142. El control de privacidad 164 tiene una copia en caché 144 del Perfil de privacidad 152 del dispositivo inalámbrico 100. Esto permite el procesamiento de la verificación de privacidad en el servidor de red 140 para las solicitudes de acceso del servidor web 160. La comunicación entre el servidor web 160 y el servidor de red 140 se asegura utilizando los protocolos seguros de Internet, como HTTPS o SSL. El servidor de inferencia de contexto 174 puede publicar su propio servicio como servicio web para otros servicios web en Internet, en cuyo caso la implementación de la interfaz 186 entre el servidor web 160 y el servidor de red 140 puede ser mensajes de lenguaje de marcado extensible (XML) transportados en el protocolo de mensajería del Protocolo simple de acceso a objetos (SOAP).

El motor de inferencia de contexto 142 en el servidor de red 140 recibirá información procesada del vector de metadatos del sensor 138 y posiblemente alguna información de API de aplicación originada en el motor de inferencia de contexto 136 del dispositivo inalámbrico 100. El motor de inferencia de contexto 142 del servidor de red tiene una base de datos de usuario 146 con información del comportamiento del usuario y del uso pasado del dispositivo inalámbrico. El motor de inferencia de contexto 142 del servidor de red también puede tener servicios de terceros disponibles (como instancias que ofrecen contenido y/o servicios) para ofrecer a los usuarios potenciales. Lo que se ofrece al usuario también puede depender del perfil de usuario 144. La naturaleza de la información del motor de inferencia de contexto 136 del dispositivo inalámbrico 100 que se transmite al motor de inferencia de contexto 142 de la red puede controlarse con el control de privacidad 150 que es administrado por el usuario del dispositivo inalámbrico 100. De este modo, el usuario puede deshabilitar total o parcialmente el motor de inferencia de contexto 142 de la red para controlar la cantidad de su información que puede ser utilizada por servicios de terceros. El control de privacidad 150 permite al usuario controlar el acceso de cualquier persona a su información privada.

El motor de inferencia de contexto 136 del dispositivo inalámbrico recibe una entrada de la interfaz API 154 de las aplicaciones A, B, X o Y ubicadas en el dispositivo inalámbrico 100. Un ejemplo sería de un programa de aplicación de calendario que indica que una reunión está comenzando dentro de 25 minutos. Como otro ejemplo, el programa de aplicación de calendario indica que Lisa tiene un cumpleaños mañana en el que participas. El motor de inferencia de contexto 136 del dispositivo inalámbrico puede transmitir información procesada de resultados al motor de inferencia de contexto 142 del servidor de red. Ahora, además de la información del sensor, la información de los programas de aplicación A, B, X o Y también se puede utilizar en la toma de decisiones del Motor de inferencia de contexto 136 del dispositivo inalámbrico. El motor de inferencia de contexto 136 puede procesar una combinación de la información del sensor y la información proveniente de los programas de aplicación A, B, X o Y. El comportamiento del usuario o los patrones de uso pueden detectarse desde el sensor y registrarse en la base de datos del usuario, en relación con el uso de los programas de aplicación. Como se discutió anteriormente, el procesamiento de esta información combinada de los sensores y de los programas de aplicación se puede compartir entre el Motor de inferencia de contexto 136 y el Motor de inferencia de contexto 142. Los programas de aplicación A, B, X o Y que se ejecutan en el dispositivo inalámbrico 100 o los programas de aplicación de servidor A, X e Y que se ejecutan en el servidor web 160, pueden proporcionar opcionalmente datos de aplicación al motor de inferencia de contexto 142 en el servidor de red 140. El motor de inferencia de contexto 142 puede procesar opcionalmente el vector de metadatos 138 y los datos de la aplicación para producir el contexto actual.

La transferencia de información desde el motor de inferencia de contexto 136 del dispositivo inalámbrico al motor de inferencia de contexto 142 del servidor de red se puede hacer de formas alternativas. El sistema se puede gestionar de modo que se tenga en cuenta el consumo actual y la capacidad de transferencia entre el dispositivo inalámbrico 100 y el servidor de red 140. La información de contexto no siempre tiene que recopilarse con tanta frecuencia que debería transferirse periódicamente al lado de la red 140 cada pocos segundos. Dependiendo de la aplicación, la ventana de tiempo aplicada a la transferencia de información desde el Motor de inferencia de contexto 136 del dispositivo inalámbrico 100 al Motor de inferencia de contexto 142 del servidor 140 puede variar de segundos a minutos. Si no hubiera ningún cambio de evento o cambio de condición en el entorno del dispositivo inalámbrico 100, no habría necesidad de transferir información al Motor de inferencia de contexto 142 del servidor 140. Además, la información puede almacenarse temporalmente en una memoria intermedia en el dispositivo inalámbrico 100, que luego puede transferirse con menos frecuencia al motor de inferencia de contexto de red 142. Los paquetes GPRS y UMTS basados en paquetes pueden soportar las tasas de transferencia de información menos frecuentes. Además, es ventajoso enviar la información del motor de inferencia de contexto de red 142 desde el dispositivo inalámbrico 100 como un archivo adjunto, inmediatamente posterior a otra señalización realizada en la dirección de la red desde el dispositivo inalámbrico 100, guardando así el transmisor de radio del dispositivo inalámbrico 100 de tener que volver a encenderlo para transferir la información del motor de inferencia de contexto 136 por separado al servidor de red 140.

Volviendo a la figura 1, se muestra la relación entre el servidor de red 140, el registro 170 de Descripción Universal, Descubrimiento e Integración (UDDI) y una pluralidad de servidores de sitio web 160. UDDI es un estándar de facto para un registro basado en Internet. El registro UDDI 170 permite que el servidor de red 140 descubra nuevos sitios web para servicios y negocios en Internet. Una vez que dichos servicios y negocios son identificados por el registro 170 UDDI al servidor de red 140, entonces el servidor 140 debe aplicar el perfil de privacidad en caché 144 del usuario móvil en la figura 2A, para evitar el acceso no autorizado de los datos privados del usuario por los programas de aplicación en los sitios web recién descubiertos.

La figura 3 es un diagrama de flujo del proceso de red de la interacción del dispositivo inalámbrico 100 l en la primera columna, el servidor de red 140 en la columna central y el servidor web 160 en la columna derecha, cuando llevan a cabo la determinación del contexto actual del dispositivo inalámbrico 100. El proceso comienza con el dispositivo inalámbrico 100 en la etapa 302:
Etapa 302: CONTROL DE PRIVACIDAD 150 EN DISPOSITIVO INALÁMBRICO 100 ENVÍA PERFIL DE PRIVACIDAD ACTUALIZADO AL SERVIDOR DE RED 140.

Entonces el servidor de red 140 continúa con la etapa 304:
Etapa 304: SERVIDOR DE RED 140 ACTUALIZA PERFIL DE PRIVACIDAD EN CACHÉ 144.

El dispositivo inalámbrico 100 continúa con las siguientes etapas 306, 308 y 310:

Etapa 306: LOS SENSORES PROPORCIONAN CONTINUAMENTE DATOS DEL SENSOR PARA CONTEXTAR EL MOTOR DE INFERENCIA 136 EN EL DISPOSITIVO INALÁMBRICO 100.

Etapa 308: EL PROGRAMA DE APLICACIÓN QUE UTILIZA CONOCIMIENTO DE CONTEXTO API 154 SOLICITA LA ÚLTIMA INFORMACIÓN DE CONTEXTO.

Etapa 310: MOTOR DE INFERENCIA DE CONTEXTO 136 CONTACTO MOTOR DE INFERENCIA DE CONTEXTO 142 DEL SERVIDOR DE RED 140 Y ENVÍA EL VECTOR DE METADATOS 138 AL SERVIDOR 140.

Luego, el servidor de red 140 continúa con las etapas 312 y 314:

Etapa 312: EL MOTOR DE INFERENCIA DE CONTEXTO 142 EN EL SERVIDOR DE RED 140 UTILIZA LA INFORMACIÓN LOCAL DEL USUARIO ALMACENADA EN LA BASE DE DATOS DEL USUARIO 146 PARA HACER UNA DETERMINACIÓN MÁS EXACTA DEL CONTEXTO ACTUAL DEL USUARIO MÓVIL.

Etapa 314: SERVIDOR DE RED 140 SOLICITA DATOS DEL SERVIDOR WEB 160.

EL ACCESO DEL SERVIDOR DE RED ESTÁ AUTORIZADO POR EL PERFIL DE PRIVACIDAD EN CACHÉ 144 EN EL SERVIDOR DE RED.

Luego el servidor web 160 continúa con la etapa 316:
Etapa 316: EL SERVIDOR WEB PROPORCIONA INFORMACIÓN DEL USUARIO ALMACENADA EN LA BASE DE DATOS 184 AL SERVIDOR DE RED 140.

Entonces el servidor de red 140 continúa con la etapa 318:
Etapa 318: EL MOTOR DE INFERENCIA DE CONTEXTO 142 EN EL SERVIDOR DE RED 140 ENTONCES DEVUELVE SEGURAMENTE LA INFORMACIÓN ACTUAL DE CONOCIMIENTO DE CONTEXTO AL MOTOR DE INFERENCIA DE CONTEXTO 136 EN EL DISPOSITIVO INALÁMBRICO 100.

Entonces el dispositivo inalámbrico 100 termina con la etapa 320:
Etapa 318: EL MOTOR DE INFERENCIA DE CONTEXTO 136 EN EL DISPOSITIVO INALÁMBRICO 100 ENTONCES PROPORCIONA LA INFORMACIÓN ACTUAL DE CONOCIMIENTO DE CONTEXTO A TRAVÉS DE LAS API DE CONOCIMIENTO DE CONTEXTO 154 A LOS PROGRAMAS DE APLICACIÓN REGISTRADOS PARA RECIBIR ESTA INFORMACIÓN.

La figura 4 es un diagrama de bloques funcional del servidor de red 140, que muestra la memoria 402 que almacena los programas de software de servicios de aplicaciones necesarios para realizar las operaciones de la invención. La memoria está conectada por el bus 404 al caché 144, la base de datos de usuario 146, el adaptador de red TCP/IP 406 y el procesador central 410. La memoria 402 almacena programas que son secuencias de instrucciones ejecutables que, cuando se ejecutan por el procesador 410, llevan a cabo los métodos de la invención.

La figura 4 es un diagrama de bloques funcional del servidor de red, que muestra la memoria que almacena los programas de software de servicios de aplicaciones necesarios para realizar las operaciones de una realización de la invención. La figura 4 describe los componentes funcionales de un servidor de red 140 a modo de ejemplo dispuesto como un modelo de objeto. El modelo de objetos agrupa los programas de software orientados a objetos en

componentes que realizan las principales funciones y aplicaciones en el servidor de red 140. El modelo de objetos para la memoria 402 del servidor de red 140 emplea una arquitectura de tres niveles que incluye el nivel de presentación 415, la partición de objetos de infraestructura 422 y el nivel de lógica de negocios 414. El modelo de objetos divide además el nivel 414 de lógica de negocios en dos particiones, la partición de objetos de aplicación 422 y la partición de objetos de datos 426.

El nivel de presentación 415 retiene los programas que administran las interfaces del dispositivo al servidor de red 140. En la figura 4, el nivel de presentación 415 incluye la interfaz de red 420. Una implementación adecuada del nivel de presentación 415 puede usar servlets Java para interactuar con la puerta de enlace de protocolo WAP 120 a través del protocolo de transferencia de hipertexto ("HTTP"). Los servlets de Java se ejecutaron dentro de un servidor de solicitud/respuesta que gestiona el intercambio de mensajes entre la puerta de enlace de protocolo WAP 120 y el servidor de red 140. Un servlet Java es un programa Java que se ejecuta dentro de un entorno de servidor web. Un servlet Java toma una solicitud como entrada, analiza los datos, realiza operaciones lógicas y emite una respuesta a la puerta de enlace de protocolo WAP 120. La plataforma de tiempo de ejecución de Java agrupa los servlets de Java para atender simultáneamente muchas solicitudes. La interfaz de red 420 acepta mensajes de solicitud de la puerta de enlace de protocolo WAP 120 y pasa la información en la solicitud para visitar el objeto 428 para su posterior procesamiento. El objeto de visita 428 pasa el resultado de ese procesamiento a la interfaz de red 420 para la transmisión de regreso a la puerta de enlace de protocolo WAP 120. La interfaz de red 420 también puede usar el adaptador de red 406 para intercambiar datos con otro dispositivo de usuario.

La partición de objetos de infraestructura 422 retiene los programas que realizan funciones administrativas y del sistema en nombre del nivel 414 de lógica de negocios. La partición de objetos de infraestructura 422 incluye el sistema operativo 425 y un componente de programa de software orientado a objetos para la interfaz del servidor de la base de datos 430 y la interfaz del administrador del sistema 432.

El nivel 414 de lógica de negocios en la figura 4 incluye varias instancias del objeto de visita 428, 428', 428". Existe una instancia separada del objeto de visita 428 para cada sesión de la interfaz de red 420. Cada objeto de visita 428 es un objeto de sesión con estado que incluye un área de almacenamiento persistente desde el inicio hasta la finalización de la sesión, no solo durante una sola interacción o llamada al método. El área de almacenamiento persistente retiene la información asociada con la sesión.

Cuando la puerta de enlace de protocolo WAP 120 envía un mensaje de vector de metadatos 138 al servidor de red 140, el mensaje se envía a la interfaz de red 420 para invocar un método que crea el objeto de visita 428 y almacena información de conexión como un estado en el objeto de visita 428. El objeto de visita 428 puede, a su vez, invocar un método en la aplicación 440 del motor de inferencia de contexto 142 para realizar una inferencia de contexto en el vector de metadatos y devolver un resultado de contexto actual.

Cuando la puerta de enlace de protocolo WAP 120 envía un mensaje de datos de control de privacidad 150’ al servidor de red 140, el mensaje se envía a la interfaz de red 420 para invocar un método que crea el objeto de visita 428 y almacena información de conexión como un estado en el objeto de visita 428. El objeto de visita 428 puede, a su vez, invocar un método en la aplicación 442 de control de privacidad 164 para actualizar el perfil de privacidad en caché 144. La aplicación 442, a su vez, hace una llamada al método para la aplicación de actualización del perfil de privacidad 448 para almacenar los datos actualizados 150’ en el caché 144.

Cuando la puerta de enlace de protocolo WAP 120 envía un mensaje de actualización de datos de usuario al servidor de red 140, el mensaje se envía a la interfaz de red 420 para invocar un método que crea el objeto de visita 428 y almacena la información de conexión como un estado en el objeto de visita 428. El objeto de visita 428 puede, a su vez, invocar un método en la aplicación de base de datos de usuario 446 para almacenar los datos de usuario en la base de datos 146.

Ed Roman proporciona una descripción de las aplicaciones de programación de servidores desarrolladas con Enterprise Java Beans en el libro titulado "Mastering Enterprise Java Beans", publicado por John Wiley and Sons, 1999. En el libro de Matthew Reynolds titulado "Beginning E-Commerce", Wrox Press Inc, 2000, (ISBN: 1861003986), se proporciona una descripción del uso de un modelo de objetos en el diseño de aplicaciones de servidor. Los servlets de Java y el desarrollo de servidores de sitios web se describen en el libro de Duane K. Fields, et al. titulado "Web Development with Java Server Pages", publicado por Manning Publications Co., 2000.

La invención de servicios web sensibles al contexto resultante permite que un teléfono móvil o dispositivo inalámbrico 100 use técnicas de inferencia de contexto para detectar el entorno del usuario y, en respuesta, proporcionar información útil para el usuario que sea apropiada para el entorno percibido del usuario. El usuario móvil tiene la capacidad de controlar el acceso de los programas de aplicación a cualquier lugar de la red a los datos privados del usuario.

REIVINDICACIONES

1. Un método que comprende:

recibir, en un dispositivo inalámbrico (100), señales de sensor que caracterizan una o más condiciones ambientales, que incluyen al menos una primera señal y una segunda señal;
combinar la al menos primera señal y la segunda señal en un vector de metadatos (138);
procesar el vector de metadatos, con un motor de inferencia de contexto (136) en el dispositivo inalámbrico, para determinar un resultado de contexto actual;
generar el resultado del contexto actual del procesamiento;
anexar a un programa de aplicación (106), una autorización para acceder al resultado del contexto actual;
otorgar permiso de acceso al programa de aplicación para acceder al resultado del contexto actual basado en la autorización;
proporcionar el resultado del contexto actual al programa de aplicación basado en la concesión del permiso de acceso; y recibir información del programa de aplicación que depende del resultado del contexto actual.

2. El método de la reivindicación 1, en el que el vector de metadatos se relaciona con un estado de salud y/o fatiga de un usuario, y/o en donde la información recibida del programa de aplicación se relaciona con un estado de salud y/o fatiga de un usuario.

3. El método de cualquiera de las reivindicaciones 1 a 2, que comprende además enviar el vector de metadatos a un servidor de red separado (140) para el procesamiento adicional del vector de metadatos dentro del servidor de red separado (140).

4. El método de la reivindicación 3, en el que el dispositivo inalámbrico (100) descarga una parte del procesamiento del vector de metadatos al servidor (140).

5. El método de las reivindicaciones 3 o 4, en el que el procesamiento adicional, dentro del servidor de red separado, del vector de metadatos comprende el procesamiento del vector de metadatos, con un motor de inferencia de contexto (142) en el servidor de red separado, para determinar el resultado del contexto actual;
comprendiendo el método además recibir, en el dispositivo inalámbrico, el resultado del contexto actual del servidor de red separado.

6. El método de la reivindicación 5, que comprende adicionalmente:

enviar, al motor de inferencia de contexto en el servidor de red separado, datos de aplicación desde un programa de aplicación en el dispositivo inalámbrico; y
recibir, en el dispositivo inalámbrico, el resultado del contexto actual del servidor de red separado, en donde el procesamiento por el motor de inferencia de contexto (142) en el servidor de red separado para determinar el resultado del contexto actual comprende procesar el vector de metadatos y los datos de la aplicación.

7. El método de la reivindicación 1, que comprende adicionalmente:

recibir datos de la aplicación de un programa de aplicación en el dispositivo inalámbrico; y
procesar el vector de metadatos y los datos de la aplicación recibidos del programa de aplicación, con el motor de inferencia de contexto (136) en el dispositivo inalámbrico, para determinar el resultado del contexto actual.

8. El método de la reivindicación 1, en el que al menos las señales primera y segunda se reciben desde los al menos primer y segundo sensores respectivamente;
aplicar una ponderación a las al menos primera y segunda señales dependiendo de un valor de peso de los al menos primer y segundo sensores respectivamente;
en donde el motor de inferencia de contexto adapta continuamente el valor de peso del primer y segundo sensores a través de métodos de aprendizaje adaptativo y continuo.

9. El método de la reivindicación 1, que comprende adicionalmente:
proporcionar a un usuario control de acceso sobre el resultado del contexto actual a aplicaciones y servicios sensibles al contexto dentro de un servidor de red (140).

10. Un dispositivo inalámbrico (100) que comprende:

un procesador (210);
una memoria (202) acoplada al procesador, programada para realizar las etapas de:

recibir señales del sensor que caracterizan una o más condiciones ambientales, que incluyen al menos una primera señal y una segunda señal;
combinar la al menos primera señal y la segunda señal en un vector de metadatos (138);

procesar el vector de metadatos, con un motor de inferencia de contexto (136) en el dispositivo inalámbrico, para determinar un resultado de contexto actual;
generar el resultado del contexto actual del procesamiento;
anexar a un programa de aplicación (106), una autorización para acceder al resultado del contexto actual;
otorgar permiso de acceso al programa de aplicación para acceder al resultado del contexto actual basado en la autorización;
proporcionar el resultado del contexto actual al programa de aplicación basado en la concesión del permiso de acceso; y recibir información del programa de aplicación que depende del resultado del contexto actual.

11. El dispositivo inalámbrico de la reivindicación 10, en el que la memoria (202) está programada además para realizar las etapas de cualquiera de las reivindicaciones 2 a 9.

12. Un dispositivo inalámbrico móvil, un teléfono móvil o un asistente digital personal inalámbrico que comprende el dispositivo inalámbrico de las reivindicaciones 10 u 11.

13. Un sistema, que comprende:

un dispositivo inalámbrico (100) según se reivindica en las reivindicaciones 10 u 11;
uno o más sensores para proporcionar al menos una primera señal de sensor y una segunda señal de sensor que caracterizan una o más condiciones ambientales; y
un servidor (140).

14. El sistema de la reivindicación 13, en el que el servidor (140) comprende un procesador (410), en donde el procesador (410) está configurado para ejecutar instrucciones almacenadas en una memoria (402) para procesar el vector de metadatos para determinar el resultado del contexto actual; y en donde el servidor (140) está dispuesto para recibir el vector de metadatos enviado desde el dispositivo inalámbrico (100) y completar un procesamiento del vector de metadatos.

15. Un programa informático que, cuando es ejecutado por al menos un procesador (210), hace que se realice el método según se reivindica en una cualquiera o más de las reivindicaciones 1 a 9.

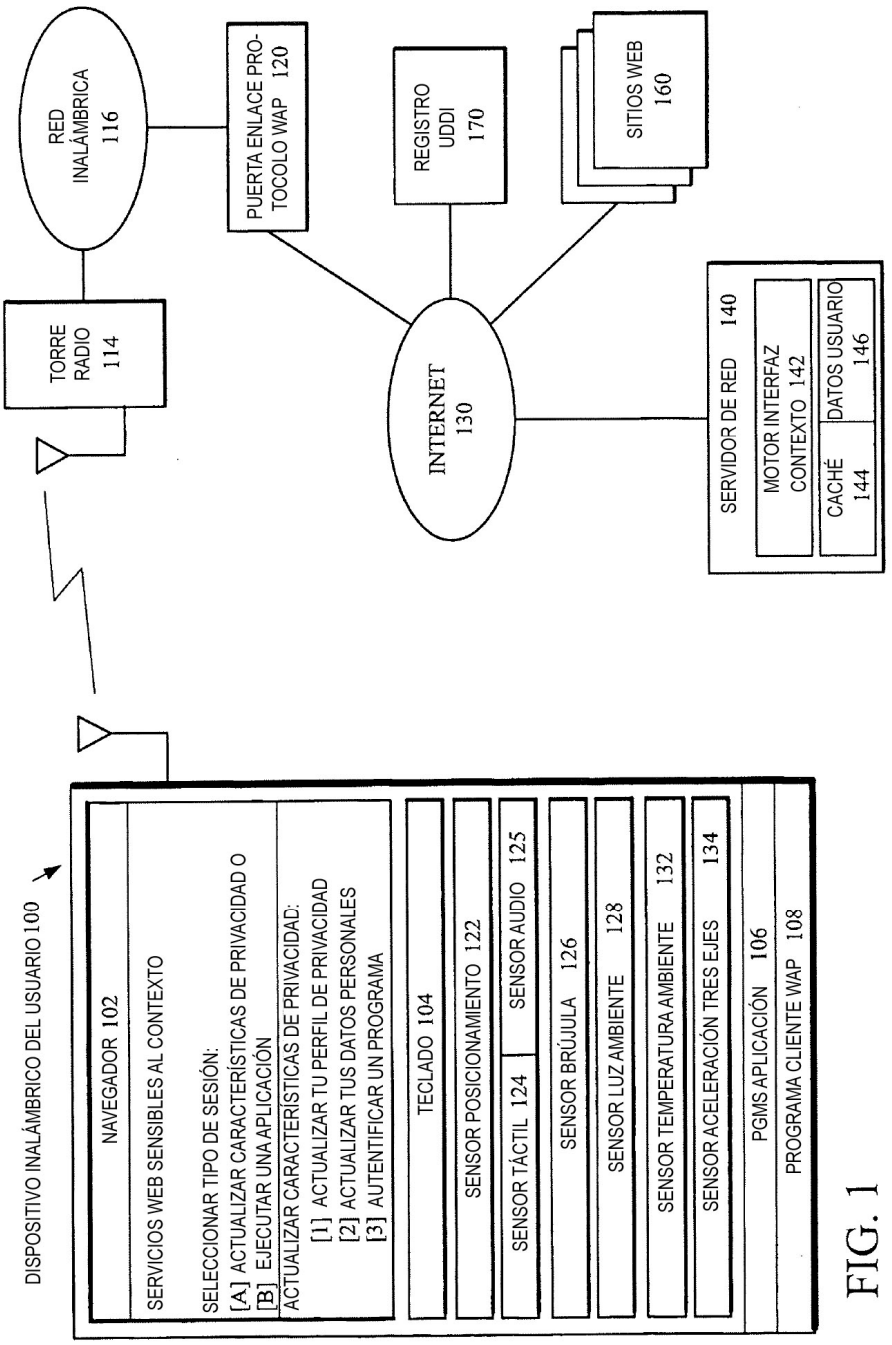

DISPOSITIVO INALÁMBRICO DEL USUARIO 100
NAVEGADOR 102
SERVICIOS WEB SENSIBLES AL CONTEXTO
SELECCIONAR TIPO DE SESIÓN:
[A] ACTUALIZAR CARACTERÍSTICAS DE PRIVACIDAD O
[B] EJECUTAR UNA APLICACIÓN
ACTUALIZAR CARACTERÍSTICAS DE PRIVACIDAD:
[1] ACTUALIZAR TU PERFIL DE PRIVACIDAD
[2] ACTUALIZAR TUS DATOS PERSONALES
[3] AUTENTIFICAR UN PROGRAMA
TECLADO 104
SENSOR POSICIONAMIENTO 122
SENSOR TÁCTIL 124
SENSOR AUDIO 125
SENSOR BRÚJULA 126
SENSOR LUZ AMBIENTE 128
SENSOR TEMPERATURA AMBIENTE 132
SENSOR ACELERACIÓN TRES EJES 134
PGMS APLICACIÓN 106
PROGRAMA CLIENTE WAP 108
TORRE RADIO 114
RED INALÁMBRICA 116
PUERTA ENLACE PROTOCOLO WAP 120
INTERNET 130
REGISTRO UDDI 170
SITIOS WEB 160
SERVIDOR DE RED 140
MOTOR INTERFAZ CONTEXTO 142
CACHÉ 144
DATOS USUARIO 146

FIG. 1

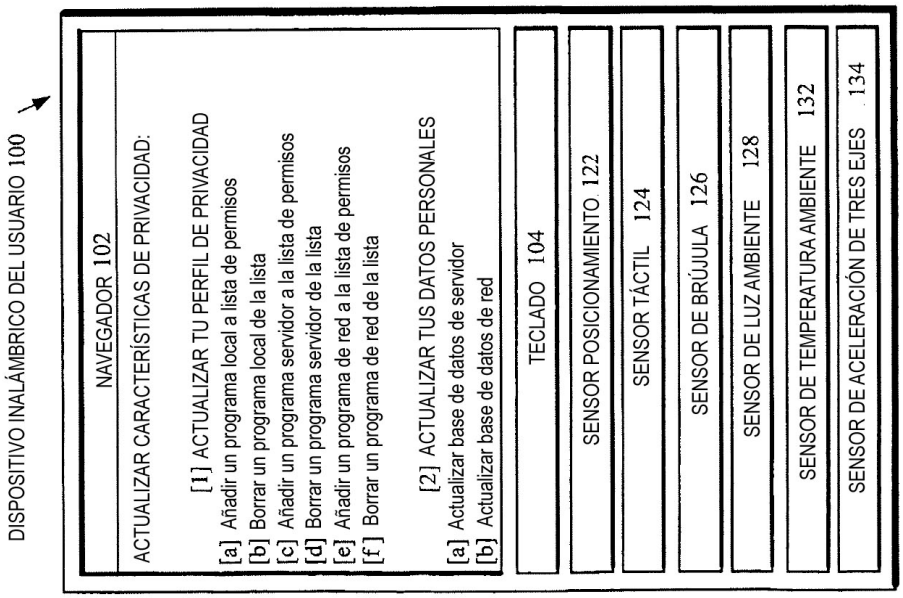

DISPOSITIVO INALÁMBRICO DEL USUARIO 100
NAVEGADOR 102
ACTUALIZAR CARACTERÍSTICAS DE PRIVACIDAD:
[1] ACTUALIZAR TU PERFIL DE PRIVACIDAD
[a] Añadir un programa local a lista de permisos
[b] Borrar un programa local de la lista
[c] Añadir un programa servidor a la lista de permisos
[d] Borrar un programa servidor de la lista
[e] Añadir un programa de red a la lista de permisos
[f] Borrar un programa de red de la lista
[2] ACTUALIZAR TUS DATOS PERSONALES
[a] Actualizar base de datos de servidor
[b] Actualizar base de datos de red
TECLADO 104
SENSOR POSICIONAMIENTO 122
SENSOR TÁCTIL 124
SENSOR DE BRÚJULA 126
SENSOR DE LUZ AMBIENTE 128
SENSOR DE TEMPERATURA AMBIENTE 132
SENSOR DE ACELERACIÓN DE TRES EJES 134

FIG. 1A

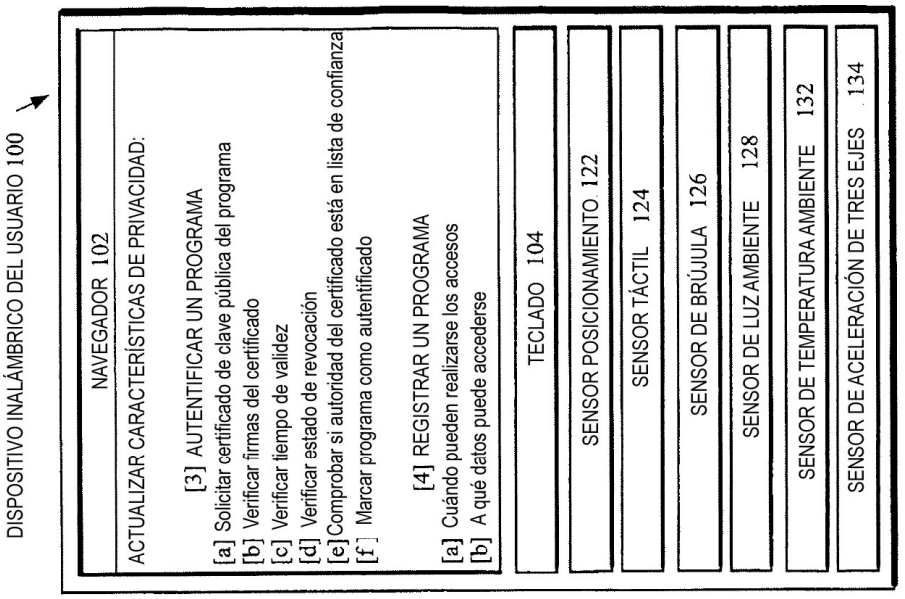

DISPOSITIVO INALÁMBRICO DEL USUARIO 100
NAVEGADOR 102
ACTUALIZAR CARACTERÍSTICAS DE PRIVACIDAD:
[3] AUTENTIFICAR UN PROGRAMA
[a] Solicitar certificado de clave pública del programa
[b] Verificar firmas del certificado
[c] Verificar tiempo de validez
[d] Verificar estado de revocación
[e] Comprobar si autoridad del certificado está en lista de confianza
[f] Marcar programa como autentificado
[4] REGISTRAR UN PROGRAMA
[a] Cuándo pueden realizarse los accesos
[b] A qué datos puede accederse
TECLADO 104
SENSOR POSICIONAMIENTO 122
SENSOR TÁCTIL 124
SENSOR DE BRÚJULA 126
SENSOR DE LUZ AMBIENTE 128
SENSOR DE TEMPERATURA AMBIENTE 132
SENSOR DE ACELERACIÓN DE TRES EJES 134

FIG. 1B

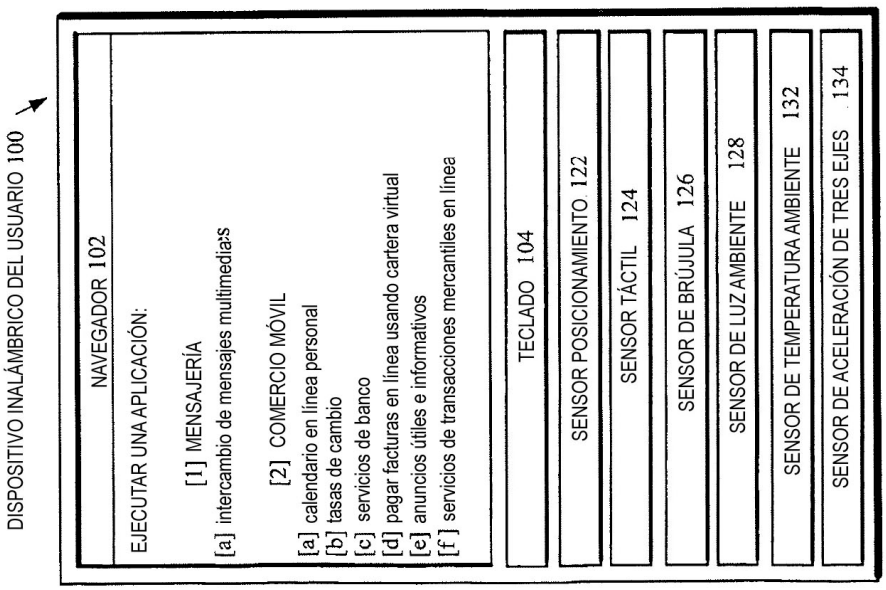

DISPOSITIVO INALÁMBRICO DEL USUARIO 100
NAVEGADOR 102
EJECUTAR UNA APLICACIÓN:
[1] MENSAJERÍA
[a] intercambio de mensajes multimedia:s
[2] COMERCIO MÓVIL
[a] calendario en línea personal
[b] tasas de cambio
[c] servicios de banco
[d] pagar facturas en línea usando cartera virtual
[e] anuncios útiles e informativos
[f] servicios de transacciones mercantiles en línea
TECLADO 104
SENSOR POSICIONAMIENTO 122
SENSOR TÁCTIL 124
SENSOR DE BRÚJULA 126
SENSOR DE LUZ AMBIENTE 128
SENSOR DE TEMPERATURA AMBIENTE 132
SENSOR DE ACELERACIÓN DE TRES EJES 134

FIG. 1C

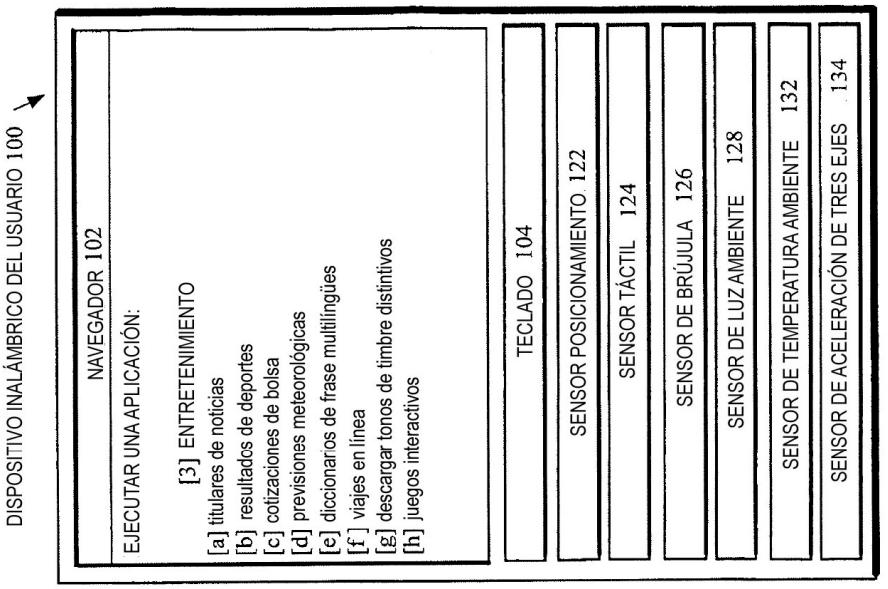

DISPOSITIVO INALÁMBRICO DEL USUARIO 100
NAVEGADOR 102
EJECUTAR UNA APLICACIÓN:
[3] ENTRETENIMIENTO
[a] titulares de noticias
[b] resultados de deportes
[c] cotizaciones de bolsa
[d] previsiones meteorológicas
[e] diccionarios de frase multilingües
[f] viajes en línea
[g] descargar tonos de timbre distintivos
[h] juegos interactivos
TECLADO 104
SENSOR POSICIONAMIENTO 122
SENSOR TÁCTIL 124
SENSOR DE BRÚJULA 126
SENSOR DE LUZ AMBIENTE 128
SENSOR DE TEMPERATURA AMBIENTE 132
SENSOR DE ACELERACIÓN DE TRES EJES 134

FIG. 1D

FIG. 2

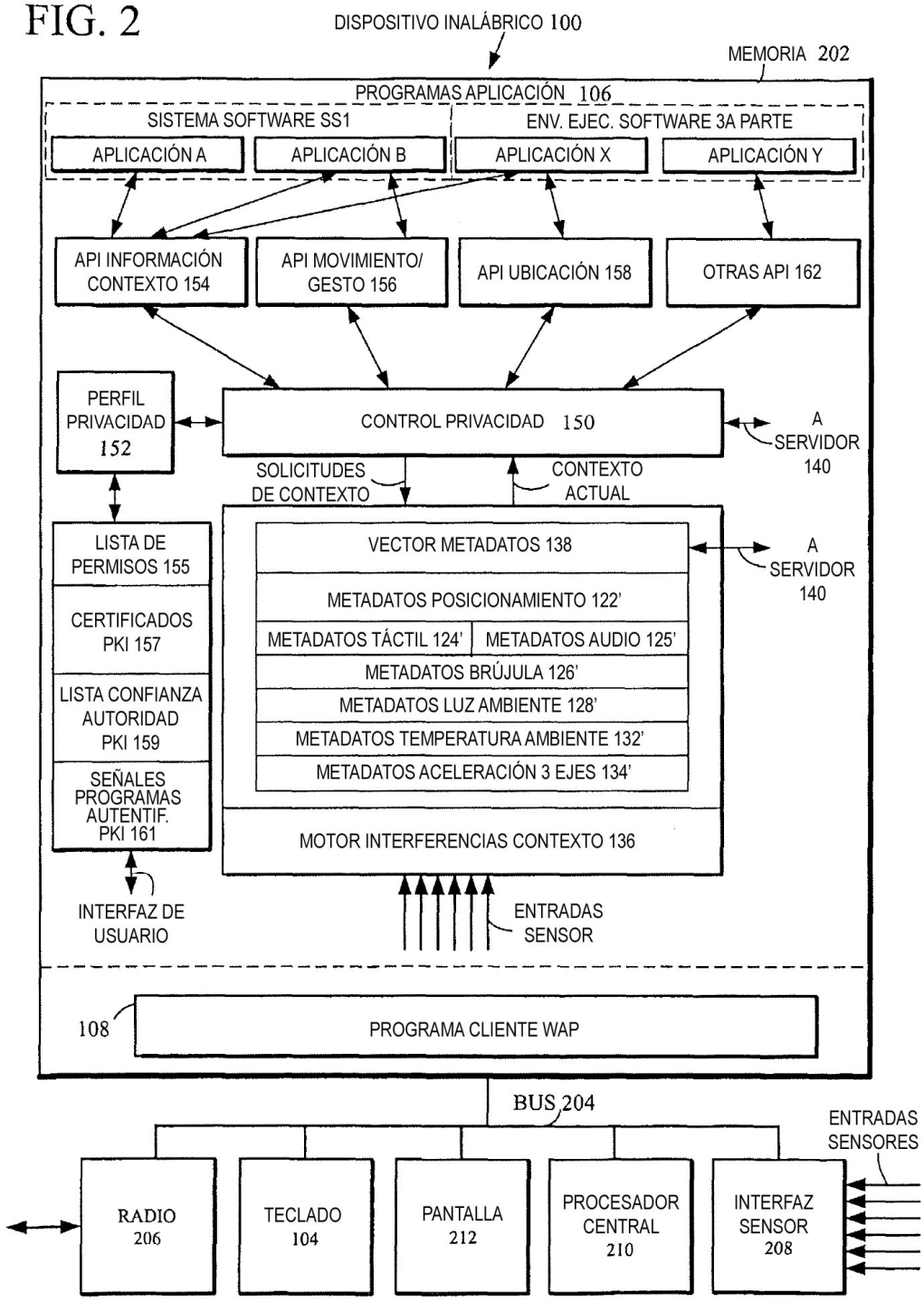

DISPOSITIVO INALÁBRICO 100
MEMORIA 202
PROGRAMAS APLICACIÓN 106
SISTEMA SOFTWARE SS1
ENV. EJEC. SOFTWARE 3A PARTE
APLICACIÓN A
APLICACIÓN B
APLICACIÓN X
APLICACIÓN Y
API INFORMACIÓN CONTEXTO 154
API MOVIMIENTO/ GESTO 156
API UBICACIÓN 158
OTRAS API 162
PERFIL PRIVACIDAD 152
CONTROL PRIVACIDAD 150
A SERVIDOR 140
SOLICITUDES DE CONTEXTO
CONTEXTO ACTUAL
LISTA DE PERMISOS 155
CERTIFICADOS PKI 157
LISTA CONFIANZA AUTORIDAD PKI 159
SEÑALES PROGRAMAS AUTENTIF. PKI 161
VECTOR METADATOS 138
A SERVIDOR 140
METADATOS POSICIONAMIENTO 122'
METADATOS TÁCTIL 124'
METADATOS AUDIO 125'
METADATOS BRÚJULA 126'
METADATOS LUZ AMBIENTE 128'
METADATOS TEMPERATURA AMBIENTE 132'
METADATOS ACELERACIÓN 3 EJES 134'
MOTOR INTERFERENCIAS CONTEXTO 136
INTERFAZ DE USUARIO
ENTRADAS SENSOR
108
PROGRAMA CLIENTE WAP
BUS 204
ENTRADAS SENSORES
RADIO 206
TECLADO 104
PANTALLA 212
PROCESADOR CENTRAL 210
INTERFAZ SENSOR 208

FIG. 2A

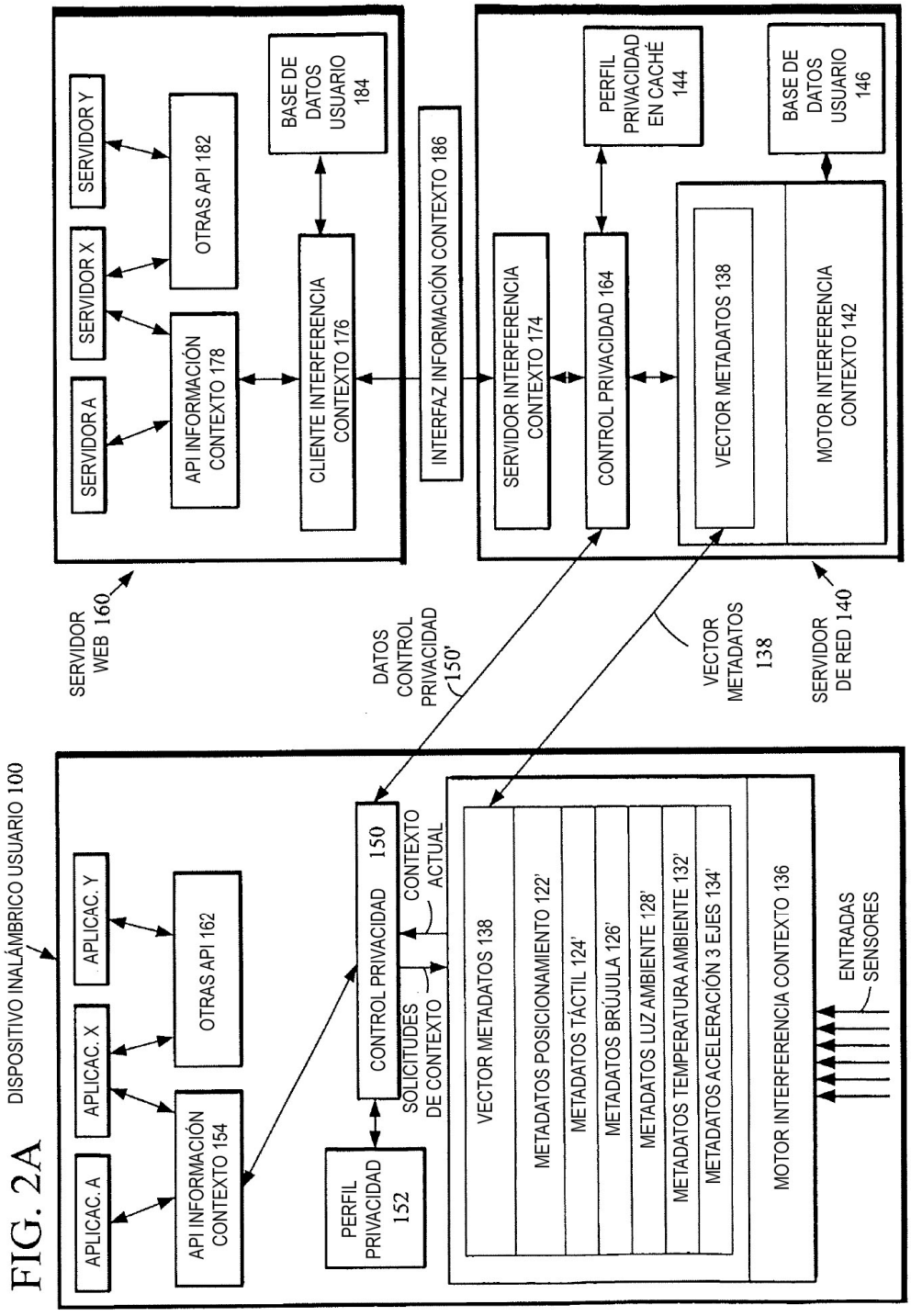

DISPOSITIVO INALÁMBRICO USUARIO 100
APLICAC. A
APLICAC. X
APLICAC. Y
API INFORMACIÓN CONTEXTO 154
OTRAS API 162
PERFIL PRIVACIDAD 152
CONTROL PRIVACIDAD 150
SOLICITUDES DE CONTEXTO
CONTEXTO ACTUAL
VECTOR METADATOS 138
METADATOS POSICIONAMIENTO 122'
METADATOS TÁCTIL 124'
METADATOS BRÚJULA 126'
METADATOS LUZ AMBIENTE 128'
METADATOS TEMPERATURA AMBIENTE 132'
METADATOS ACELERACIÓN 3 EJES 134'
MOTOR INTERFERENCIA CONTEXTO 136
ENTRADAS SENSORES
DATOS CONTROL PRIVACIDAD 150'
VECTOR METADATOS 138
SERVIDOR DE RED 140
SERVIDOR WEB 160
SERVIDOR A
SERVIDOR X
SERVIDOR Y
API INFORMACIÓN CONTEXTO 178
OTRAS API 182
CLIENTE INTERFERENCIA CONTEXTO 176
BASE DE DATOS USUARIO 184
INTERFAZ INFORMACIÓN CONTEXTO 186
SERVIDOR INTERFERENCIA CONTEXTO 174
CONTROL PRIVACIDAD 164
PERFIL PRIVACIDAD EN CACHÉ 144
VECTOR METADATOS 138
MOTOR INTERFERENCIA CONTEXTO 142
BASE DE DATOS USUARIO 146

FIG. 3

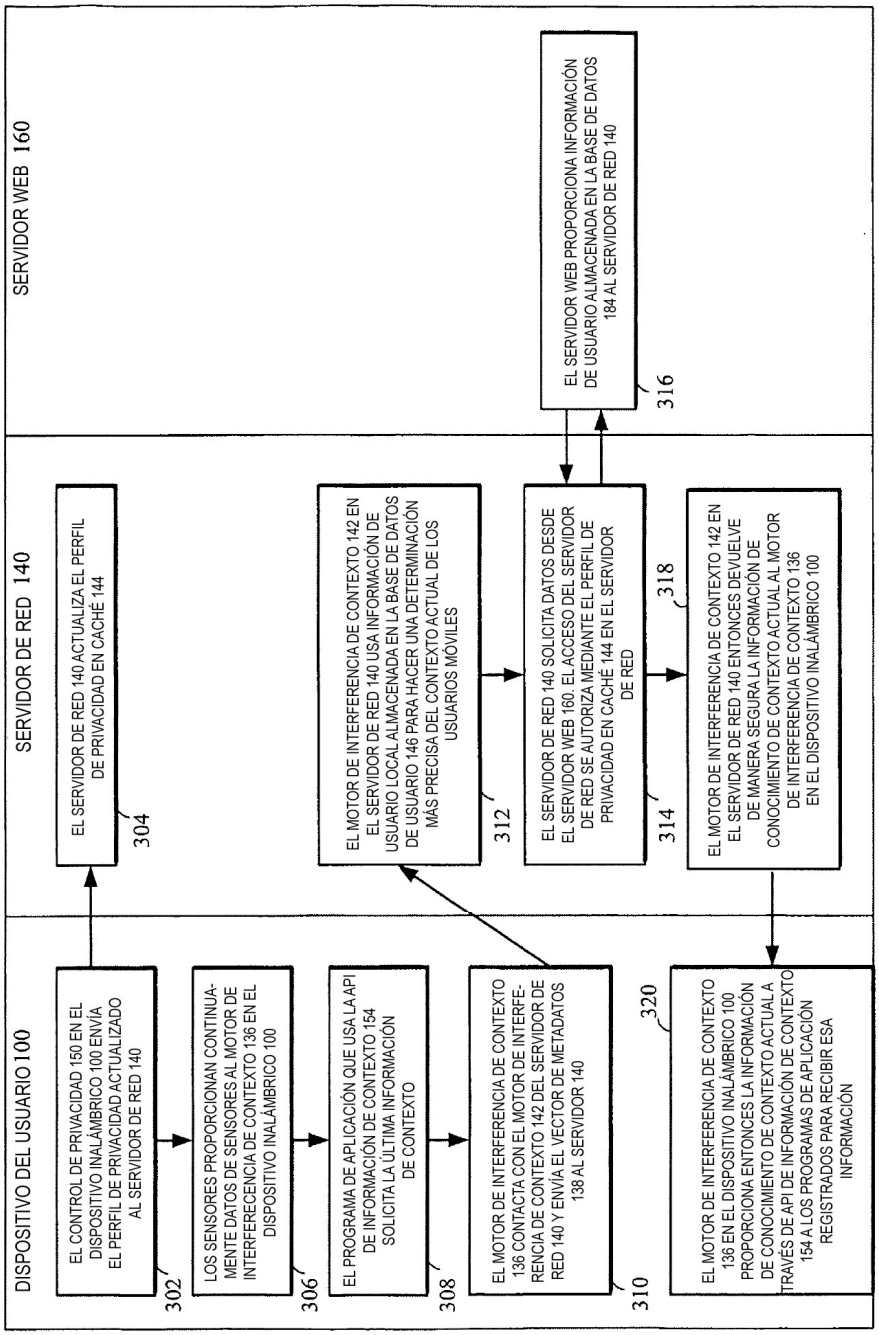
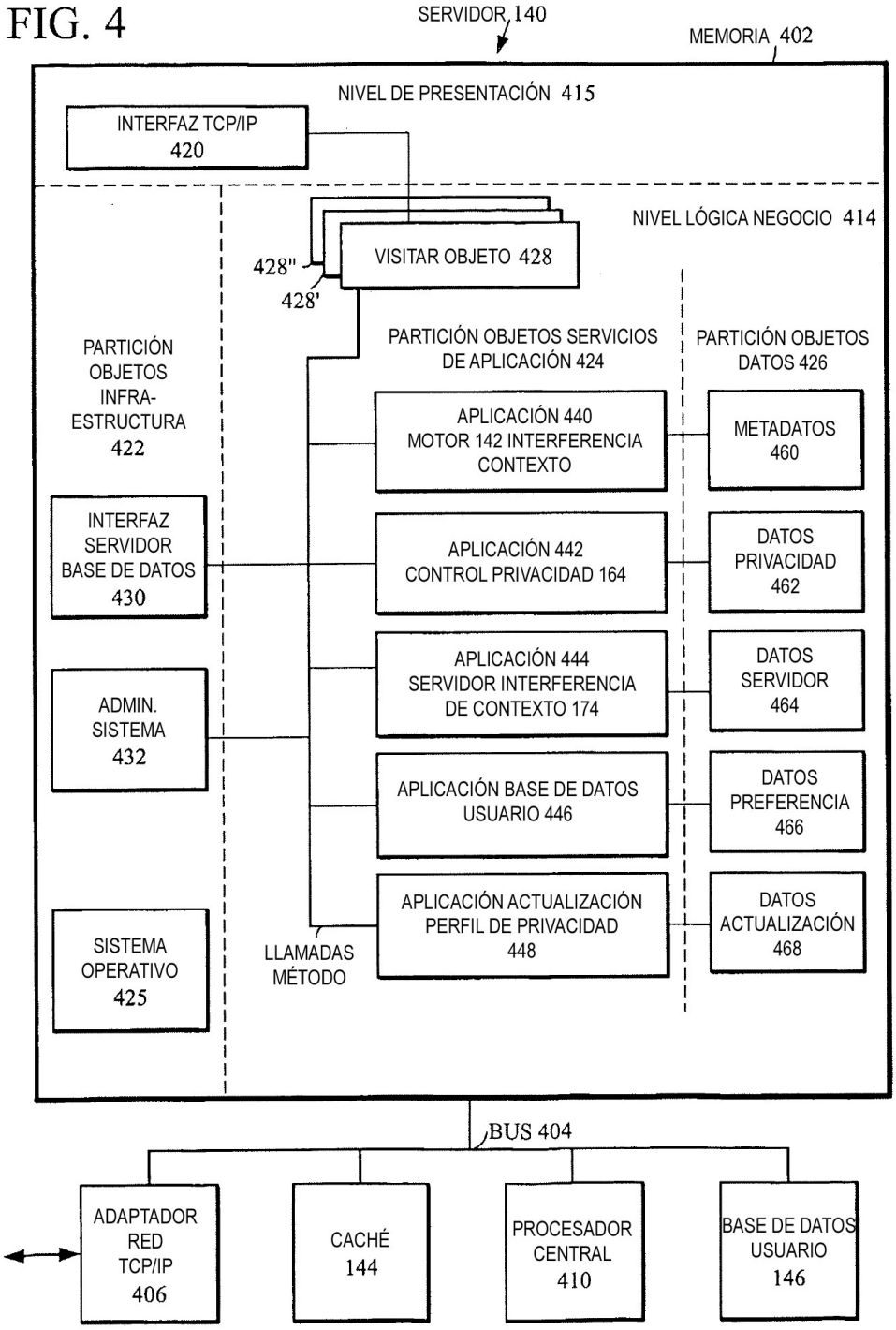

DISPOSITIVO DEL USUARIO 100
SERVIDOR DE RED 140
SERVIDOR WEB 160
EL CONTROL DE PRIVACIDAD 150 EN EL DISPOSITIVO INALÁMBRICO 100 ENVÍA EL PERFIL DE PRIVACIDAD ACTUALIZADO AL SERVIDOR DE RED 140
302
EL SERVIDOR DE RED 140 ACTUALIZA EL PERFIL DE PRIVACIDAD EN CACHÉ 144
304
LOS SENSORES PROPORCIONAN CONTINUAMENTE DATOS DE SENSORES AL MOTOR DE INTERFERECENCIA DE CONTEXTO 136 EN EL DISPOSITIVO INALÁMBRICO 100
306
EL PROGRAMA DE APLICACIÓN QUE USA LA API DE INFORMACIÓN DE CONTEXTO 154 SOLICITA LA ÚLTIMA INFORMACIÓN DE CONTEXTO
308
EL MOTOR DE INTERFERENCIA DE CONTEXTO 136 CONTACTA CON EL MOTOR DE INTERFERENCIA DE CONTEXTO 142 DEL SERVIDOR DE RED 140 Y ENVÍA EL VECTOR DE METADATOS 138 AL SERVIDOR 140
310
EL MOTOR DE INTERFERENCIA DE CONTEXTO 136 EN EL DISPOSITIVO INALÁMBRICO 100 PROPORCIONA ENTONCES LA INFORMACIÓN DE CONOCIMIENTO DE CONTEXTO ACTUAL A TRAVÉS DE API DE INFORMACIÓN DE CONTEXTO 154 A LOS PROGRAMAS DE APLICACIÓN REGISTRADOS PARA RECIBIR ESA INFORMACIÓN
320
EL MOTOR DE INTERFERENCIA DE CONTEXTO 142 EN EL SERVIDOR DE RED 140 USA INFORMACIÓN DE USUARIO LOCAL ALMACENADA EN LA BASE DE DATOS DE USUARIO 146 PARA HACER UNA DETERMINACIÓN MÁS PRECISA DEL CONTEXTO ACTUAL DE LOS USUARIOS MÓVILES
312
EL SERVIDOR DE RED 140 SOLICITA DATOS DESDE EL SERVIDOR WEB 160. EL ACCESO DEL SERVIDOR DE RED SE AUTORIZA MEDIANTE EL PERFIL DE PRIVACIDAD EN CACHÉ 144 EN EL SERVIDOR DE RED
314
EL SERVIDOR WEB PROPORCIONA INFORMACIÓN DE USUARIO ALMACENADA EN LA BASE DE DATOS 184 AL SERVIDOR DE RED 140
316
EL MOTOR DE INTERFERENCIA DE CONTEXTO 142 EN EL SERVIDOR DE RED 140 ENTONCES DEVUELVE DE MANERA SEGURA LA INFORMACIÓN DE CONOCIMIENTO DE CONTEXTO ACTUAL AL MOTOR DE INTERFERENCIA DE CONTEXTO 136 EN EL DISPOSITIVO INALÁMBRICO 100
318

FIG. 4


SERVIDOR 140
MEMORIA 402
NIVEL DE PRESENTACIÓN 415
INTERFAZ TCP/IP 420
NIVEL LÓGICA NEGOCIO 414
VISITAR OBJETO 428
428"
428'
PARTICIÓN OBJETOS INFRA-ESTRUCTURA 422
PARTICIÓN OBJETOS SERVICIOS DE APLICACIÓN 424
PARTICIÓN OBJETOS DATOS 426
APLICACIÓN 440 MOTOR 142 INTERFERENCIA CONTEXTO
METADATOS 460
INTERFAZ SERVIDOR BASE DE DATOS 430
APLICACIÓN 442 CONTROL PRIVACIDAD 164
DATOS PRIVACIDAD 462
APLICACIÓN 444 SERVIDOR INTERFERENCIA DE CONTEXTO 174
DATOS SERVIDOR 464
ADMIN. SISTEMA 432
APLICACIÓN BASE DE DATOS USUARIO 446
DATOS PREFERENCIA 466
APLICACIÓN ACTUALIZACIÓN PERFIL DE PRIVACIDAD 448
DATOS ACTUALIZACIÓN 468
SISTEMA OPERATIVO 425
LLAMADAS MÉTODO
BUS 404
ADAPTADOR RED TCP/IP 406
CACHÉ 144
PROCESADOR CENTRAL 410
BASE DE DATOS USUARIO 146