PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIONES

TESIS:

DISEÑO DE UNA RED CON TECNOLOGÍA SENSOR CLOUD APLICADA EN PREVENCIÓN DE ACCIDENTES DE TRÁNSITO

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN REDES DE COMUNICACIONES

AUTOR:

TIRIRA CALUQUÍ PAOLA ELIZABETH

DIRECTOR:

DR. GUSTAVO CHAFLA

QUITO, MAYO 2017

AGRADECIMIENTOS

Agradezco a Dios, por estar presente en mi vida a través de las personas que amo.

A mis padres por su apoyo incondicional.

A Marcelo, por apoyarme y ayudarme en todo momento.

A esta noble institución y al personal docente y administrativo, en especial al Dr. Gustavo Chafla, director de tesis, quien ha sabido brindarme su valiosa ayuda y experiencia.

A mis revisores de tesis MSc. Juan Francisco Chafla y MSc. Francisco Rodríguez por sus amplios conocimientos técnicos y profesionales.

A mis hermanos que supieron darme una palabra de aliento, gracias por compartir su experiencia.

Paola

DEDICATORIA

A mis padres, por su ejemplo y apoyo incondicional durante mi carrera y toda mi vida. Gracias por estar siempre a mi lado, brindándome su amor, cariño y comprensión.

Gracias por inculcarme los mejores valores y el sentido de la responsabilidad y de la lucha constante para sacar adelante las metas propuestas.

A mi Marcelito por la ayuda, paciencia y apoyo incondicional, gracias mi amor, me enseñas a sonreírle a la vida cada día.

A mis hermanos por demostrarme que la vida vale la pena vivirla y por inculcarme el deseo de superación con su ejemplo, gracias por su confianza.

A mis sobrinos Brianna y Alejandro por ser fuente de mi alegría.

Paola

RESUMEN

La red con tecnología sensor cloud para prevención de accidentes de tránsito diseñada puede ser aplicada en el entorno de monitoreo vial por las entidades que se encargan del control y monitoreo de la seguridad vial, cuyo objetivo es minimizar la ocurrencia de accidentes de tránsito que sean ocasionadas por factores emocionales del conductor, como lo son el estrés y el cansancio; tales variables emocionales pueden ser determinadas mediante un algoritmo que evalúa variables como la temperatura, equilibrio (sensor de mercurio) y datos de una cámara de video (expresiones faciales), que mediante algoritmos de procesamiento implementados en una plataforma cloud computing permiten la determinación de emociones del conductor y seguidamente la toma de decisiones para activar una alarma o la visualización de un mensaje en una pantalla instalada en el vehículo para que el conductor tome las acciones necesarias que permitan precautelar su vida y la de sus pasajeros; mejorando y optimizando de esta manera los sistemas de monitoreo vial.

La red de sensores inalámbrica puede ser implementada con tecnología ZigBee o 6LoWPAN, basadas en el estándar IEEE 802.15.4 haciendo posible que los nodos de la red se conecten a la nube mediante su coordinador respectivo, además de un gateway que actúa como interfaz hacia la nube, específicamente hacia una aplicación SaaS que hace uso de toda la información enviada por los sensores para determinar principalmente el estado emocional del conductor.

Para la recolección de las mediciones de la red, se utiliza el estándar IEEE 802.15.4, y para el envío de datos del Gateway a la nube se plantea un

esquema de publicación/ suscripción con un módulo de gestión de identidad y acceso para control de la seguridad del sistema mediante políticas de acceso determinadas, además de un servidor web que gestiona el almacenamiento.

Como parte final de la investigación, se plantean las conclusiones y recomendaciones, en las cuales se exponen los resultados obtenidos de la investigación y las recomendaciones para futuros estudios.

Palabras clave: *WSN, Cloud computing, 6LowPAN, Sensor Cloud.*

CONTENIDO

INDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPITULO I:

INTRODUCCIÓN DEL PROYECTO DE INVESTIGACIÓN

1.1Introducción

En los últimos años, las redes de sensores inalámbricos (WSNs) se han posicionado como una tecnología que permite adaptar el ambiente físico al mundo digital. Los nodos de sensores de manera cooperada monitorean condiciones en diferentes ubicaciones, tales como temperatura, humedad, movimiento vehicular, condiciones de luz, presión, niveles de ruido, presencia o ausencia de ciertos tipos de objetos, además de características como: velocidad, dirección, tamaño de objetos. Los nodos de sensores son pequeños, de bajo consumo, bajo costo y proveen múltiples funcionalidades como capacidad de detección, procesamiento de energía, memoria, ancho de banda para comunicaciones y consumo de batería, estas se utilizan en varias aplicaciones tales como: medición de parámetros del medio ambiente, cuidado de la salud, educación, defensa, manufactura, casas inteligentes o domótica. La meta principal se resume en facilitar la conexión de sensores, personas y objetos para construir una comunidad centralizada con aplicaciones de medición de parámetros, donde las personas puedan compartir y analizar datos de sensores en tiempo real. Por ejemplo las instituciones públicas que planifican, regulan y controlan el transporte terrestre, tránsito y seguridad vial y que tienen como objetivo incrementar el nivel de seguridad vial, lograrían prevenir accidentes de tránsito mediante el monitoreo en tiempo real de los vehículos de transporte público. Para obtener datos en tiempo real se instalaría en las unidades de transporte biosensores y una cámara de video, los cuales enviarían una serie de datos en tiempo real para su respectivo almacenamiento y procesamiento en la nube de

sensores, los datos permitirán realizar el reconocimiento de las expresiones faciales y análisis de las variables fisiológicas para determinar el estado de ánimo del conductor, según el cual se tomarán acciones inmediatas para controlar esta variable, mediante una alarma sonora o una pantalla led se explicaría acciones a tomarse por parte del conductor o del pasajero, inclusive se puede llevar a cabo una ambientación automática del interior del vehículo e informar a las unidades de emergencia según sea el caso.

Se requiere un servicio escalable, confiable y disponible para proveer información en tiempo real relacionada a presión, temperatura, tráfico, cuidado de la salud, seguridad en el transporte público, estadísticas del medio ambiente, para lo cual las redes de sensores son las mejores alternativas, sin embrago, los principales cuellos de botella de la tecnología de redes de sensores inalámbricos son la energía de la batería disponible para procesamiento local y el tamaño de la memoria.

La integración de Cloud Computing a la infraestructura de red de sensores inalámbricos, resuelve los inconvenientes presentados ya que proporciona recursos confiables, software y datos bajo demanda, permitiendo la observación y el intercambio de datos a largo plazo además de innovar en servicios de aplicación.

La infraestructura de la nube de sensores Sensor Cloud es la forma extendida de computación en la nube, con funcionalidades para gestionar sensores que se encuentran dispersos a lo largo de las redes de sensores inalámbricos WSN, en general el modelo Cloud Sensor permite el intercambio de datos de sensores en tiempo real a través de Cloud Computing.

1.2 Justificación e Importancia

Actualmente se observa un incremento en el número creciente de sensores físicos usados para varios propósitos, los cuales están conectados a sus propios sistemas de TI, sin embargo, ahora es necesario una infraestructura en la cual los usuarios sean capaces de acceder a diferentes tipos de sensores físicos. La infraestructura Sensor Cloud tiene la capacidad de administrar sensores físicos en una infraestructura de TI como un sensor virtual en la nube de computación.

Entre los objetivos que persigue la infraestructura Sensor Cloud está incrementar la disponibilidad de información de un sensor en tiempo real, además permite compartir información de redes de sensores de aplicaciones específicas de diferentes ubicaciones.

La importancia de este proyecto radica en que la tecnología Sensor Cloud permite utilizar los datos de sensores para servicios de aplicación de siguiente generación, las redes de sensores monitorean, recogen y envían información a la nube la cual ofrece el almacenamiento y procesamiento necesario. El desarrollo de estos sistemas da una mayor flexibilidad a la ejecución de consultas de diferentes redes que constan de diferentes tipos de dispositivos con varios lenguajes de programación, lo cual permite la integración de redes.

Con la ayuda de técnicas de virtualización, transparencia, escalabilidad y seguridad se mantiene en la plataforma de la nube. La arquitectura sugerida provee virtualización entre sensores frente a la nube y la nube frente a los usuarios. La plataforma mejorará el cuello de botella de procesamiento de sensores a través del procesamiento en tiempo real de los datos de los sensores en recursos de la nube para ponerlo a disposición de

la comunidad que lo necesite. Además, esto facilitará la interoperabilidad de las redes de sensores desplegados para su aplicación específica.

Ha habido estudios en la gestión de sensores físicos, en general se indica que los usuarios necesitan saber las especificaciones de diferentes tipos de sensores físicos, OGC (Open Geoespatial Consortium) es una organización internacional sin fines de lucro que desarrolla de forma colaborativa estándares de interfaz y los estándares asociados, así como buenas prácticas, que permiten a los desarrolladores crear sistemas de información que pueden fácilmente intercambiar información geográfica e instrucciones con otros sistemas de información. La organización se encuentra comprometida con la difusión de estándares para la comunidad geoespacial global.

OGC define el lenguaje sensor modeling SensorML, para proveer modelos estándar y una codificación XML para descripción y medición de procesos de sensores físicos.

SensorML puede representar los metadatos para cualquier sensor físico (tal como el tipo de sensor físico, la ubicación, y la precisión). Utilizamos SensorML para describir los metadatos de sensores físicos. Se Añade el mapeo entre sensores físicos y sensores virtuales para describir cómo traducir los comandos procedentes de los usuarios a los sensores virtuales en comandos para los correspondientes sensores físicos.

Aunque hay muchos tipos de sensores físicos, ninguna aplicación necesita utilizar todos ellos. Cada aplicación necesita sensores físicos suficientes para sus necesidades (por ejemplo, sensores físicos en un lugar determinado). Para seleccionar los sensores físicos se utiliza un mecanismo de publicación/suscripción. Cuando hay varias redes de sensores, cada red de sensores publica datos de los sensores y los metadatos que

describen el tipo de sensores físicos. Cada aplicación se suscribe a una o más redes de sensores para recibir un flujo de datos en tiempo real de sus sensores físicos.

1.3 Antecedentes

La revolución de la tecnología está cambiando dramáticamente el estilo de vida de las personas, desde la introducción de las computadoras, las cuales tenían capacidad para procesar información por lotes en tiempo real, y que han continuado evolucionando ofreciendo cada vez mejores prestaciones, sin embargo los computadores comunes no tenían la capacidad de una unidad central en términos de proporcionar información en tiempo real. La arquitectura cliente-servidor provee mejor rendimiento con menor costo de mantenimiento y complejidad; este modelo es de alta disponibilidad y escalabilidad, la arquitectura está formada por un servidor de base de datos centralizado e interfazado con los computadores personales. Sin embargo, el principal inconveniente de estos sistemas se refiere a la disponibilidad de un servicio de información global para el usuario y para la organización. Internet resuelve esta limitación en mayor medida. Podemos visualizar a Internet como un conjunto de recursos (hardware, software e información, etc.) que tienen capacidad para ser compartida entre los usuarios que la soliciten. Sin embargo, el presente proceso de Internet carece de almacenamiento, memoria y dispositivos de procesamiento de alta velocidad. Esta restricción dio inicio a un modelo reciente conocido como ''computación en la nube '' que puede proporcionar recursos abundantes en términos de información y recursos de computación. Cloud Computing se clasifica en tres modelos de servicio: software como servicio (SaaS), infraestructura como servicio (IaaS), y plataforma como servicio (PaaS). SaaS ofrece servicios de software en la nube, eliminándose la necesidad de instalar y ejecutar la

aplicación en la computadora propia del cliente. IaaS facilita el acceso a servidores virtualizados, hardware y redes. PaaS entrega una plataforma de computación como servicio, este facilita el desarrollo de aplicaciones sin costo y sin la complejidad de comprar y gestionar capas de hardware y software.

La disponibilidad de información en tiempo real es crítica en aplicaciones como monitoreo de la salud, monitoreo del medio ambiente, monitoreo de vehículos, entre otros.

En conclusión la nube ofrece inmenso poder de cómputo y almacenamiento, el beneficio máximo en redes de sensores se puede lograr mediante la integración de las redes de sensores con la nube, lo cual corresponde al paradigma Sensor Cloud.

1.4 Objetivos

1.4.1 Objetivo General

Diseñar una red con tecnología Sensor Cloud como propuesta de integración en instituciones que controlan el transporte público, tránsito y seguridad vial, para prevención de accidentes de tránsito, optimización de la seguridad vial, monitoreo en tiempo real y acceso a los datos fisiológicos y de estado emocional a largo plazo a través de Internet.

1.4.2 Objetivos Específicos

- Describir las características, plataforma, protocolos, estándares y arquitectura de la tecnología Sensor Cloud.
- Realizar un análisis comparativo de las tecnologías idóneas para desarrollo de aplicaciones en prevención de accidentes de tránsito en base a los requerimientos establecidos.
- Diseñar la arquitectura de Sensor Cloud para una aplicación en prevención de accidentes de tránsito, tomando en cuenta los siguientes componentes: plataforma de sensores usable, una estación conductor, un servidor central, un servidor de la nube, un servidor de almacenamiento, un servidor de comunicaciones.
- Optimizar la plataforma de monitoreo de las instituciones de seguridad vial, mediante el diseño de una alternativa tecnológicamente viable, con almacenamiento y procesamiento virtual en la nube.

CAPITULO II

FUNDAMENTO TEÓRICO

2.1Fundamentos y Características principales de redes de sensores inalámbricos (WSN)

2.1.1 Definición

Una red de sensores (del inglés sensor network) es una red de diminutos dispositivos, equipados con sensores, que colaboran en una tarea común. Las redes de sensores están formadas por un grupo de sensores con ciertas capacidades sensitivas y de comunicación inalámbrica que permiten formar redes ad-hoc sin infraestructura física preestablecida ni administración central. (Roberto Fernández, 2009)

Las redes inalámbricas de sensores (WSN - Wireless Sensor Network), se basan en dispositivos de bajo coste y consumo (nodos) que son capaces de obtener información de su entorno, procesarla localmente, y comunicarla a través de enlaces inalámbricos hasta un nodo central de coordinación. Los nodos actúan como elementos de la infraestructura de comunicaciones al reenviar los mensajes transmitidos por nodos más lejanos hacia al centro de coordinación. (ESEC, 2014)

2.1.2 Arquitectura del Sistema WSN

2.1.2.1 Nodo Inalámbrico

Los nodos inalámbricos se llaman motas, del inglés ‘mote’, por su ligereza y reducido tamaño. Son dispositivos electrónicos capaces de captar información proveniente del entorno en el que se encuentran, procesarla y transmitirla inalámbricamente hacia otro

destinatario. El hardware de estos dispositivos está formado por: procesador, alimentación, comunicación inalámbrica (radio- transceptor RF), sensor, memoria. (Roberto Fernández, 2009) (Surya Bharat, 2014)

1. Un subsistema de detección para la adquisición de datos del medio ambiente circundante (sensor).
2. Un subsistema de procesamiento para el procesamiento de datos local (procesador).
3. Un subsistema de comunicación inalámbrica para la transmisión de datos (comunicación inalámbrica /radio- transceptor RF).
4. Una batería que suministra toda la energía necesaria para el funcionamiento (alimentación).
5. Una memoria para almacenar los datos recogidos (memoria).

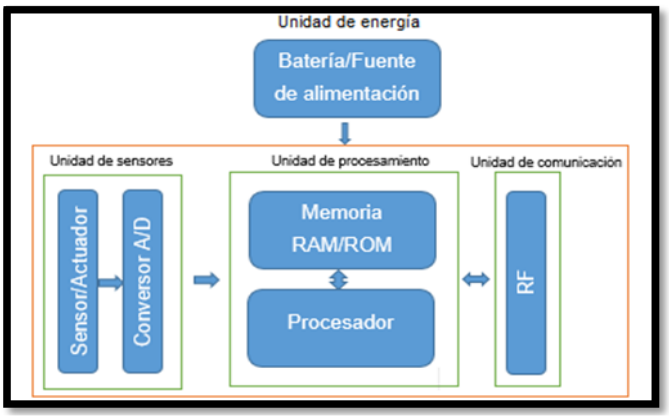


Figura 1. Arquitectura de un nodo sensor

Fuente: (Maya, 2014)

A continuación se explica cada uno de los componentes:

- **Procesador:**

Es el componente que interpreta y procesa los datos para transmitirlos a otra estación. También gestiona el almacenamiento de datos en la memoria. Es utilizado en tareas de

procesamiento y manipulación de datos, almacenamiento transitorio, cifrado, corrección de errores (FEC), modulación y transmisión digital. Los requisitos de cómputo y almacenamiento en una WSN dependen de la aplicación y pueden ir desde la utilización de un microcontrolador de 8 bits hasta 64 bits. Los requerimientos de almacenamiento pueden igualmente oscilar entre 0,01 hasta 100 gigabytes (GB). (Flores, 2012)

- **Alimentación:**

Normalmente la fuente de alimentación son baterías difícilmente sustituibles o transformadores con salida adecuada para el nodo si se dispone de toma de corriente. Para las situaciones en donde no se dispone de red eléctrica y la posibilidad de sustituir las baterías es muy complicada, se están estudiando diferentes técnicas para alimentar el sensor, como puede ser mediante placas solares. (Roberto Fernández, 2009)

Ante la limitación de vida útil del dispositivo hay que realizar una gestión eficiente del consumo energético. El consumo de energía viene dado por lo que consumen los sensores, la comunicación y el procesamiento. La mayor cantidad de energía es consumida en la transmisión de la información, siendo menor en el procesamiento y uso de los sensores. (Flores, 2012)

- **Comunicación inalámbrica (Radio):**

El dispositivo de comunicación es un dispositivo vía radio que permite enviar y recibir datos para comunicarse con otros dispositivos dentro de su rango de transmisión. Los nodos usan la banda ISM que son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica. El uso de estas bandas de frecuencia está abierto a todo el mundo sin necesidad de licencia, respetando las regulaciones que limitan los niveles de potencia transmitida.

Los medios a elegir para realizar una comunicación inalámbrica son varios, radio frecuencia, comunicación óptica mediante láser e infrarrojos. (Roberto Fernández, 2009)

Proporciona comunicación inalámbrica al nodo sensor, y es compatible con las propiedades específicas de comunicación de las WSN tales como: bajo consumo de energía y velocidad de datos, y distancias cortas. (Flores, 2012)

- **Sensores:**

Los sensores son dispositivos hardware que producen una respuesta medible ante un cambio en un estado físico, como puede ser temperatura o presión. Los sensores detectan o miden cambios físicos en el área que están monitorizando. La señal analógica continua detectada es digitalizada por un convertidor analógico digital y enviada a un controlador para ser procesada. (Flores, 2012)

Las características y requerimientos que un sensor debe tener son un pequeño tamaño, un consumo bajo de energía, operar en densidades volumétricas altas, ser autónomo y funcionar desatendidamente y tener capacidad para adaptarse al ambiente. (Roberto Fernández, 2009)

- **Memoria:**

Desde un punto de gasto de energía, las clases más relevantes de memoria son la memoria integrada en el chip de un microcontrolador y la memoria flash, la memoria RAM fuera del chip es raramente usada. Las memorias flash son usadas gracias a su bajo coste y su gran capacidad de almacenamiento. (Roberto Fernández, 2009)

2.1.2.2 Gateway

Elementos para la interconexión entre la red de sensores y una red de datos (TCP/IP). Es un nodo especial sin elemento sensor, cuyo objetivo es actuar como puente entre dos redes de diferente tipo. En este tipo de aplicaciones donde se usan redes de sensores, éstas no pueden operar completamente aisladas y deben contar con alguna forma de monitoreo y acceso a la información adquirida por los nodos de la red de sensores. De aquí surge la necesidad de conectar las redes de sensores a infraestructuras de redes existentes tales como Internet, redes de área local (LAN) e intranets privadas. Los dispositivos que realizan la función de interconectar dos redes de diferente naturaleza se les llama dispositivo puerta de enlace; pero el término más conocido en el ambiente de las redes es Gateway. (Scanaill., 2013)

2.1.2.3 Estación Base

Se encarga de recolectar los datos basados en un ordenador común o sistema embebido. En una estructura normal todos los datos van a parar a un equipo servidor dentro de una base de datos, desde donde los usuarios pueden acceder remotamente, observar y estudiar los datos. (Flores, 2012)

2.1.3 Funcionamiento de la arquitectura del sistema

Se realiza una serie de mediciones sobre el medio, se transforma dicha información en digital en el propio nodo y se transmite fuera de la red de sensores vía un elemento gateway a una estación base, donde la información puede ser almacenada y tratada temporalmente para acabar finalmente en un servidor con mayor capacidad que permita componer un histórico o realizar análisis de datos. (Roberto Fernández, 2009)

2.1.4 Topologías de red

Hay varias arquitecturas que pueden ser usadas para implementar una aplicación de WSN como pueden ser estrella, malla o una híbrida entre ellas dos. Cada topología presenta desafíos, ventajas y desventajas. Para entender las diferentes topologías es necesario conocer los diferentes componentes de la WSN. (Roberto Fernández, 2009)

- **Nodos finales:** Compuesto por sensores y actuadores donde se capturan los datos sensores. Para las redes basadas en ZigBee son llamados RFD (Reduced Functional Devices). (Rodríguez, 2006)
- **Routers:** Dan cobertura a redes muy extensas pudiendo salvar obstáculos, problemas de congestión en la emisión de la información y posibles fallos en alguno de los aparatos. (Rodríguez, 2006)
- **Puertas de enlace:** Recoge los datos de la red, sirve como punto de unión con una red LAN o con Internet. (Roberto Fernández, 2009)

La topología se refiere a la configuración de los componentes hardware y como los datos son transmitidos a través de esa configuración. Cada topología es apropiada bajo ciertas circunstancias y puede ser inapropiada en otras. La idea de una red de sensores surge gracias a las posibilidades que nos da la tecnología. (Roberto Fernández, 2009)

2.1.4.1 Topología en estrella:

Una topología en estrella es un sistema donde la información enviada sólo da un salto y donde todos los nodos sensores están en comunicación directa con la puerta de enlace, usualmente a una distancia de 30 a 100 metros. (Roberto Fernández, 2009)

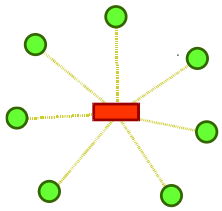


Figura 2. Topología en estrella

Fuente: (Roberto Fernández, 2009)

La topología en estrella es la que menor gasto de energía desarrolla, pero por el contrario esta limitada por la distancia de transmisión vía radio entre cada nodo y la puerta de enlace. Tampoco tiene un camino de comunicación alternativo en caso de que uno de los nodos tenga obstruido el camino de comunicación, lo que lleva a que en este caso la información de ese nodo sea perdida. (Roberto Fernández, 2009)

2.1.4.2 Topología en malla:

La topología en malla es un sistema multisalto, donde todos los nodos son routers y son idénticos. Cada nodo puede enviar y recibir información de otro nodo y de la puerta de enlace. A diferencia de la topología en estrella, donde los nodos solo pueden hablar con la puerta de enlace, en ésta los nodos pueden enviarse mensajes entre ellos. (Roberto Fernández, 2009)

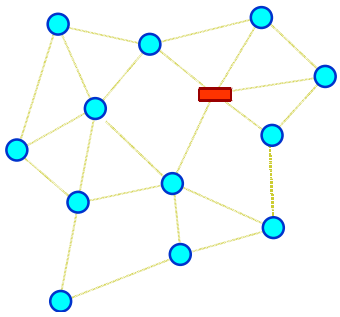


Figura 3. Topología en malla

Fuente: (Roberto Fernández, 2009)

La propagación de los datos a través de los nodos hacia la puerta de enlace hace posible, por lo menos en teoría, crear una red con una extensión posible ilimitada. Este tipo, también es altamente tolerante a fallos ya que cada nodo tiene diferentes caminos para comunicarse con la puerta de enlace. Si un nodo falla, la red se reconfigurará alrededor del nodo fallido automáticamente.

Dependiendo del número de nodos y de la distancia entre ellos, la red puede experimentar periodos de espera elevados a la hora de mandar la información. (Roberto Fernández, 2009)

2.1.4.3 Topología híbrida estrella-malla:

Este tipo de red busca combinar las ventajas de los otros dos tipos, la simplicidad y el bajo consumo de una topología en estrella, así como la posibilidad de cubrir una gran extensión y de reorganizarse ante fallos de la topología en malla. Este tipo crea una red en estrella alrededor de routers pertenecientes a una red en malla. Los routers dan la posibilidad de ampliar la red y de corregir fallos en estos nodos y los nodos finales se conectan con los routers cercanos ahorrando energía. (Roberto Fernández, 2009)

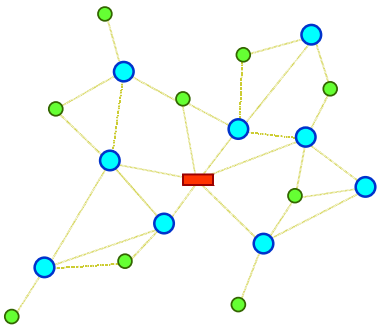


Figura 4. Topología Híbrida Malla-Estrella

Fuente: (Roberto Fernández, 2009)

2.1.5 Protocolos

La red de sensores inalámbrica para su funcionamiento requiere la inclusión de protocolos de enrutamiento que nos permitan crear las rutas hacia los destinos deseados. Los protocolos tradicionales propios de redes fijas no se adaptan bien a este tipo de entornos tan dinámicos y, por tanto, será necesario el diseño específico de protocolos para proporcionar un comportamiento eficiente a la red. (Roberto Fernández, 2009)

A diferencia de las redes inalámbricas tradicionales, las WSNs se componen de nodos con los recursos de hardware y de energía limitadas. Por lo tanto, los nodos deben utilizar protocolos de comunicación diseñados específicamente para trabajar con las fuentes de energía y los escasos recursos de hardware. Además, estos protocolos no son compatibles con los protocolos de la pila TCP/ IP. (Lucas Iacono C. G., 2013)

Existen diferentes protocolos de la capa física y la subcapa MAC para redes de sensores inalámbricos. Sin embargo, el estándar IEEE 802.15.4 se ha convertido en uno de los más populares en el campo de las redes inalámbricas de sensores. La popularidad de IEEE 802.15.4 se debe a que es fácil de implementar y totalmente cumple con los requisitos de rendimiento de WSN. Además, en los últimos años ha aumentado el número de fabricantes de hardware que proporcionan IEEE 802.15.4. Las principales aplicaciones de IEEE 802.15.4 incluyen WSNs, domótica, control de la salud, etc. (Lucas Iacono C. G., 2013)

Actualmente existen diferentes protocolos que añaden funcionalidades para IEEE 802.15.4 como ZigBee. ZigBee añade la capa de red, servicios de seguridad y subcapa soporte de aplicaciones (APS) por encima de la subcapa MAC IEEE 802.15.4. Estas características añadidas por ZigBee permiten perfiles de topologías de red de malla, seguridad y aplicación (salud, domótica, etc). (Lucas Iacono C. G., 2013)

2.1.5.1 Estándar IEEE 802.15.4 y Zigbee

Todo sistema u organización de elementos debe regir según normas que reglamenten su funcionamiento y aplicación. Las Redes de Sensores inalámbricos no son la excepción. Este tipo de sistema se comunica a través de señales de radio, por lo cual tiene asignado un espectro de la señal electromagnética para conseguir la comunicación entre los dispositivos de red. El estándar que fija las condiciones para que este enlace se produzca es el IEEE 802.15.4, existen más pero este es el estándar mas empleado. El IEEE 802.15.4 sirve de base para otras especificaciones como zigbee cuyo propósito es ofrecer una solución completa para este tipo de redes definiendo los niveles superiores de la pila de protocolos que el estándar 802.15.4 no cubre. (Flores, 2012)

2.1.5.2 Estándar IEEE 802.15.4

El estándar IEEE 802.15.4, cuya ultima revisión se aprobó en 2006, define una capa de comunicación que se encuentra en el nivel 2 (enlace de datos) del modelo OSI. Aquí las unidades de la información digital (bits) son gestionados y organizados para convertirse en impulsos electromagnéticos (ondas) en el nivel inferior, el físico. Su objetivo principal es permitir la comunicación entre dos dispositiivos. La característica más imporante de este estándar es su flexibilidad de red, bajo coste, bajo consumo de energía. (Flores, 2012)

Este estándar fue creado para llenar el hueco existente en el campo de estándares inalámbricos de baja tasa para las aplicaciones en redes de sensores. Los estádares existentes hasta el momento en el mercado estaban destinados a aplicaciones con mayores requisitos en cuanto a ancho de banda se refiere, como pueden ser videoconferencias o redes domésticas. (Rodríguez, 2006)

Los ejemplos más representativos de estas tendencias son:

- IEEE 802.11, también conocido como WIFI
- IEEE 802.15.1, conocido como Bluetooth que es una tecnología de red inalámbrica de baja potencia y baja tasa de comunicaciones punto a punto.
- IEEE 802.15.3: WPAN (Wireless Personal Area network) de alta tasa de datos. Se utiliza en aplicaciones que requieren alta tasa de datos o una gran cobertura, lo que supone soluciones complejas con elevado consumo de potencia.

Según (Rodríguez, 2006), la dificultad que surgía al emplear cualquiera de éstos estándares, era su gran consumo de energía y ancho de banda frente a la baja tasa y bajos requisitos de energía necesaria para las redes de sensores. En el caso de Bluetooth no esta diseñado para soportar la comunicación entre redes de varios nodos, por tanto, se necesita un nuevo estándar (IEEE 802.15.4) que cumpla con los siguientes criterios:

- Baja complejidad.
- Muy bajo consumo de energía.
- Baja tasa de datos.
- Radio de cobertura relaticamente pequeño.
- Uso de bandas de frecuencia sin licencia.
- Facil instalación.
- Bajo coste.

El requisito fundamental del estándar IEEE 802.15.4 es un consumo de potencia extremadamente bajo. La eficiencia energética de este protocolo reside fundamentalmente en el uso de las tramas “Beacon”, que permitan sincronizar los dispositivos de la red para que puedan permanecer en modo de ahorro de energía el mayor tiempo posible, esto supone una gran ventaha para el desarrollo WSN que

realicen tanto tareas de monitorización como de control. El inconveniente es que, debido al bajo consumo de potencia, el radio de cobertura se ve reducido. (Flores, 2012)

En la siguiente Tabla 1, se muestra una pequeña comparativa entre el estándar 802.15.4 y otros estándares como Bluetooth y Wi-Fi:

TABLA 1. COMPARATIVA ESTÁNDARES WIRELESS.

Estándar	Ancho de banda	Consumo de potencia	Ventajas	Aplicaciones
WI-FI	Hasta 54 Mbps	400mA tranmsitiendo 20mA en reposo	Gran ancho de banda	Navegar por internet, redes de ordenadores transferencia de ficheros.
BLUETOOTH	1Mbps	40mA transmitiendo 0.2mA en reposo.	Interoperatividad, sustituto del cable	Wireless USB, móviles, informátiva doméstica.
802.15.4	250Kbps	1.8 mA transmitiendo 5,1uA en reposo.	Batería de larga duración, bajo coste.	Control remoto, productos dependientes de la batería, sensores, etc.

Fuente: (IEEE, 2006)

Las frecuencias definidas por el estándar IEEE 802.15.4 se reparten entre los 27 canales disponibles y las bandas de frecuencias respectivas que se muestran en la Tabla 2. (Flores, 2012)

TABLA 2. BANDAS DE FRECUENCIA UTILIZADAS POR EL ESTÁNDAR IEEE 802.15.4.

Banda RF	Rango de frecuencias (MHz)	Tasa de datos (Kbps)	Número de canal	Área geográfica
868 Mhz	868,3	20	0 (1 canal)	Europa
915 MHz	902-928	40	1-10 (10 canales)	América, Australia
2400 MHz	2405-2480	250	11-26 (16 canales)	Todo el mundo

Fuente: (Flores, 2012)

La tecnología inalámbrica basada en IEEE 802.15.4 permite comunicaciones de corto alcance con distancias de hasta 75 m y bajo consumo; está diseñado para utilizar bandas de frecuencia sin licencia. Pueden funcionar en las bandas 868MHz, 915MHz y 2400MHz, aunque según (Flores, 2012) la banda de 2400MHz es la más utilizada por las siguientes razones:

- Uso sin licencia disponible en todo el mundo.
- Tasa de datos más alta y mayor numero de canales.
- Menor consumo de potencia (debido a que se tarde menos tiempo en enviar y recibir porque la tasa de datos es más alta)
- Banda de frecuencias comúnmente empleada en el mercado (también utilizada por Bluetooth y el estandar IEEE 802.11).

Las técnicas que utiliza este estándar explicado en el documento (IEEE, 2006) para evitar que todos los nodos emitan al mismo tiempo son:

- **CSMA-CA:** Cada nodo debe analizar la red antes de transmitir. Si la energía más alta se encuentra en un nivel especíico, el nodo espera al trnsceptor durante un tiempo al azar e intenta de nuevo.
- **GTS**: La segunda es una garantía de tiempo. Este sistema utiliza un nodo central (PAN coordinador), que da las franjas horarias de tiempo para cada uno de los nodos de modo que cualquier nodo sabe cuando tiene que transmitir.

2.1.5.3 Arquitectura del Estándar IEEE 802.15.4

La arquitectura definida en el estándar IEEE 802.15.4 (IEEE, 2006) se divide en dos niveles: capa física y subcapa MAC (junto con la subcapa LLC). El conjunto de subcapa MAC y subcapa LLC se conoce como capa de enlace de datos. La aquitectura se muestra en la Figura 5 a continuación:

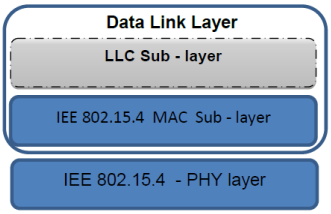


Figura 5. Arquitectura de IEEE 802.15.4

Fuente: (Flores, 2012)

A continuación se definen las funciones y servicios de ambas capas, según (Flores, 2012):

- **Capa física**

La capa física actúa como interfaz con el medio físico de transmisión, radio en este caso, e intercambia bits de datos con el medio y con la capa superior, la subcapa MAC.

Las funciones de la capa física con el medio son las siguientes:

- Estimación del canal
- Comunicaciones a nivel de bit (modulación y demodulación de bits y sincronización de paquetes).

La capa física ofrece a la subcapa MAC los siguientes servicios:

- **PHY Data Service:** proporciona un mecanismo de envío de datos a la subacapa MAC.
- **PHY Management Services:** proporciona mecanismos para controlar la configuración y la funcionalidad de las comunicaciones radio a la subcapa MAC.

La información necesaria para gestionar la capa física se almacena en una base de datos llamada PHY PIB.

- **Subcapa MAC**

Las funciones principales de la subcapa de control de acceso al medio (MAC) son las siguientes:

- Proporcionar servicios para que los dispositivos puedan asociarse o desasociarse de la red.
- Proporcionar control de acceso a los canales compartidos.
- Generación de beacons, si procede.
- Gestión de Guaranteed timeslot (GTS), si procede.

La subcapa MAC ofrece a la capa superior los siguientes servicios:

- **MAC Data Service (MCPS):** proporciona un mecanismo de envìo de datos a la capa superior.
- **MAC Management Services (MLME);** proporciona mecanismos para controlar la configuración y la funcionalidad de las comunicaciones radio y de red de la capa superior.

La información necesaria para gestionar la subcapa MAC se almacena en una base de datos llamada MAC PIB.

2.1.5.4 Zigbee

Zigbee es un conjunto de protocolos de alto nivel de comunicacion inalámbrica. Su objetivo son las aplicaciones que requieren comunicaciones seguras con baja tasa de evìo de datos y maximización de la vida útil de sus baterías. (Flores, 2012)

Fue un proyecto formado por seis promotores (honeywell, Invensys, Mitsubishi, Motorola, Philips, y Samsung y más de 80 participantes. El mismo perfil se declaró a mediados de 2003, se definieron especificaciones globales de aplicaciones

inalámbricas fiables, económicas y de baja potencia basadas en la norma IEEE 802.15.4.

Según explica (Flores, 2012) las caracteristicas básicas de ZigBee son:

- Menor potencia y menos coste que otras WPAN (como Bluetooth).
- Potencias TX 1mW (hasta 10MW en CE, hasta 100mW wn EEUU).
- Los nodos están gran parte del tiempo dormidos (larga duración. 2 años).
- Rango alcance: 10-100m, hasta 400m con 10mW.
- Bit-rate entre los 20KB/s y 250 KB/s.
- Se permiten hasta un total de 65.534 nodos /red.
- Bandas de comunicación: 868MHz, 915MHz, 2,4GHz.

2.1.5.5 Protocolos de enrutamiento para WSN

Los nodos no tienen un conocimiento de la topología de la red, deben descubrirla. La idea básica es que cuando un nuevo nodo, al aparecer en una red, anuncia su presencia y escucha los anuncios broadcast de sus vecinos. El nodo se informa acerca de los nuevos nodos a su alcance y de la manera de enrutarse a través de ellos, a su vez, puede anunciar al resto de nodos que pueden ser accedidos desde él. Transcurrido un tiempo cada nodo sabrá que nodos tiene alrededor y una o màs formas de alcanzarlos. (Flores, 2012)

Según lo expresa (Flores, 2012) en su investigación, los algoritmos de enrutamiento en redes de sensores inalámbricas tienen que cumplir las siguientes normas:

- Mantener una tabla de enrutamiento razonablemente pequeña.

- Elegir la mejor ruta para un destino dado (ya sea el màs rápido, confiable, de mejor capacidad o la ruta de menos coste)
- Mantener la tabla regularmente para actualizar la caída de nodos, su cambio de posición o su aparición
- Requerir una pequeña cantidad de mensajes y tiempo para converger.

2.1.5.6 Modelos de enrutamiento

- **Modelo de un salto**

Este es el modelo más simple y representa la comunicación directa. Todos los nodos en la red transmiten a la estación base. Es un modelo caro en términos de consumo energético, así como inviable porque los nodos tienen un rango de transmisión limitado. Sus transmisiones no pueden siempre alcanzar la estación base, tienen una distancia máxima de radio, por ello la comuncacion directa no es una buena solución para las redes inalambricas. (Flores, 2012)

- **Modelo Multihop**

En este modelo, un nodo transmite a la estación base reenviando sus datos a uno de sus vecinos, el cual esta más próximo a las estación base, a la vez que este enviará a otro nodo más próximo hasta que llegue a la mota base. Entonces la información viaja de la fuente al destino salto a salto desde un nodo a otro hasta que llega al destino. En vista de las limitaciones de los sensores es una aproximación viable. Un gran número de protocolos utilizan este modelo, entre ellos todos los Multihop Tmote Sky y Telos: Multihop LQI, MintRoute, Router, etc. (Flores, 2012)

- **Modelo esquemático basado en clústeres**

Algunos otros protocolos usan técnicas de optimización para mejorar la eficacia del modelo anterior. Una de ellas es la agregación de datos usada en todos los protocolos de enrutamiento basados en clústeres. Una aproximación esquemática rompe la red en capas de clústeres. Los nodos se agruparán en clústeres con una cabeza, la responsable de enrutar desde ese cluster a las cabezas de otros clústeres o la estación base. Los datos viajan desde un cluster de capa inferior a uno de capa superior. Aunque, salta de uno a otro, lo está haciendo de una capa a otra, por lo que cubre mayores distancias. Esto hace que además, los datos se transfieran más rápido a la estación base. (Quirasco, (2007))

Teorícamente, la latencia en este modelo es mucho menos que nen la de Multihop. El crear clústeres provee la capacidad inherente de optimización de cabezas de clúster. Por lo tanto, este modelo será mejor que los anterioresmpara redes con gran cantidad de nodos en un espacio amplio (del orden de miles de sensores y cientos de metros de distancia). (Flores, 2012)

2.1.6 Sistema operativo para nodos sensores

Como explica (Flores, 2012) las necesidades que tiene un nodo de una WSN son totalmente distintas a las que puede tener otro dispositivo como puede ser un PC, por lo tanto estos nodos tienen sus propios sistemas operativos.

Los sistemas operativos para WSN son típicamente menos complejos que los de propósito general, tanto debido a los requisitos especiales de las aplicaciones en las que se usan, como a las restricciones de recursos encontrados en las plataformas para PC y debido a esto, estos sistemas no necesitan incluir el soporte de interface de

usuario. Además, las restriccones de los recursos en términos de memoria hace imposible de implementar los mecanismos de memoria virtual.

El hardware de las redes inalámbricas de sensores no es muy diferente al de sistemas empotrados tradicionales y por lo tanto es posible utilizar sistemas como Mantis, eCos o uC/OS. Sin embargo, estos sistemas están diseñados para usar operaciones en tiempo real. A diferencia de los tradicionales sistemas operativos para sistemas empotrados, los sistemas desarrollados para redes de sensores inalámbricas no tienen como objetivo apoyar operaciones en tiempo real. (Flores, 2012)

A continuación se describe algunos sistemas operativos conocidos en el ámbito de las WSN (Quirasco, (2007)):

- Sistema Operativo TINYOS
- Sistema Operativo Contiki
- Sistema Operativo eCos
- MANTIS

2.1.7 Aplicaciones

En la investigación de (Héctor Ramos Morillo, 2010) y (Quirasco, (2007)) se explican las aplicaciones de las redes de sensores, como por ejemplo:

- Monitorización de un hábitat (para determinar la población y comportamiento de animales y plantas)
- Monitorización del medio ambiente, observación del suelo o agua
- Seguridad, detección de intrusos en un área objetivo
- El mantenimiento de ciertas condiciones físicas (temperatura, luz)

- Control de parámetros en la agricultura
- Detección de incendios, terremotos o inundaciones
- Sensorización de edificios “inteligentes”
- Control de tráfico
- Asistencia militar o civil
- Control de inventario
- Control médico
- Detección acústica

2.1.8 Red de sensores inalámbricos con IPV6

Una red de sensores está compuesta por varios motes que se encuentran esparcidos en un área determinada y para poder operar se los provee de un conjunto de protocolos y algoritmos especialmente implementados para redes de sensores, en especial el IEEE 802.15.4.

Para que una red de sensores inalámbricos (WSN) pueda conectarse en forma nativa a Internet, el IETF ha desarrollado una serie de protocolos, normalmente denominados 6LowPAN. Este simplifica las funcionalidades de protocolo de internet IPv6, definiendo un encabezamiento muy compacto y tomando en cuenta la naturaleza de las redes inalámbricas. (Carlos Taffernaberry, IETFDay 2015)

2.1.8.1 El estándar IEEE 802.15.4

El estándar IEEE 802.15.4 define las características de la capa física y de la capa de control de acceso al medio (MAC) para redes inalámbricas de área personales (WPAN, Wireless Personal Area Networks) de baja tasa de transmisión. Este estándar no establece un nivel de red pero si plantea parámetros para su implementación. Las ventajas de utilizar el estándar IEEE 802.15.4 es que permite la utilización de dispositivos de fácil instalación que proveen transmisiones confiables a distancias cortas a un precio muy bajo. Por otro lado, el estándar IEEE 802.15.4 permite proporcionar un tiempo de vida razonable al utilizar fuentes de energía limitada (e.j. baterías alcalinas) y al mismo tiempo proporciona una pila de protocolos simple. (Carlos Taffernaberry, IETFDay 2015)

2.1.8.2 El estándar 6LOWPAN

El objetivo inicial fue definir una capa de adaptación para hacer frente a las exigencias impuestas por IPv6, tales como el aumento del tamaño de la dirección y la MTU byte de 1280. Se han definido mecanismos de encapsulación y compresión de cabecera que permiten a los paquetes IPv6 ser enviados y recibidos en redes basadas en de IEEE 802.15.4 con MTU más pequeñas. La compresión produce cabeceras a veces tan pequeñas como sólo 4 bytes, mientras que al mismo tiempo permite el uso de diferentes tipos de redes de malla y gestiona la fragmentación y reensamblaje donde sea necesario. (Zach Shelby, 2010)

Para transformar la red en una aplicación de Internet de las Cosas se debe definir la tecnología de conectividad a Internet apropiada y se debe definir el tipo de dispositivo que proporcionará la interfaz entre la WSN e Internet. En primera instancia se puede usar un edge-router desarrollado sobre una plataforma diferente que haga de pasarela

entre la red y la Internet. Se debe definir la forma en que los datos producidos por los sensores serán visualizados desde Internet, determinando los protocolos más adecuados para la aplicación de toma de datos. (Carlos Taffernaberry, IETFDay 2015)

Entre los beneficios de 6loWPAN se encuentran: el fácil uso por ser un estándar abierto, confiable y estandarizado; integración transparente con internet, escalabilidad global, flujo en-to-end, el uso existente de la infraestructura de internet, uso mínimo de cogido y memoria, entre otros. (Zach Shelby, 2010)

En la investigación de (Zach Shelby, 2010) se especifica una adaptación en el formato de cabecera IPv6, permitiendo el uso de en redes inalámbricos de bajo consumo, la compresión de cabecera IPv6 y compresión de cabecera UDP. Las características del estándar permite el direccionamiento de 64 bits y 16 bits usado en 802.15.4, autoconfiguración de la red usando neighbor discovery, soporte para unicast, compresión multicast y mapeado broadcast, fragmentación de 1280 bytes MTU de IPv6 a 127 bytes en 802.15.4 y soporte para IP routing RPL.

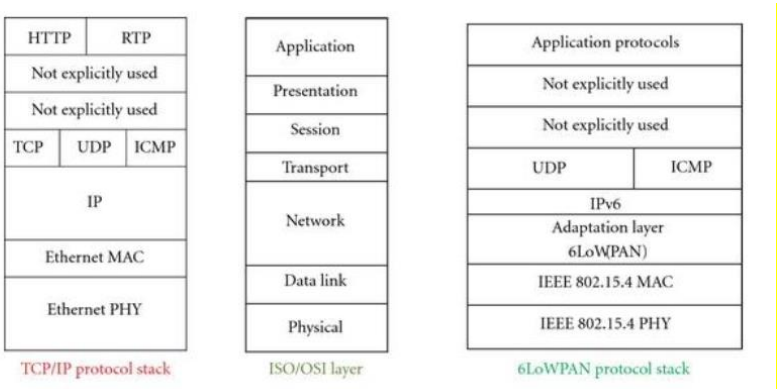


Figura 6. Comparación de la pila de TCP/IP, OSI y capa de adaptación 6loWPAN.
Fuente: (Zach Shelby, 2010)

2.1.9 Retos de enrutamiento y problemas de diseño en redes inalámbricas de sensores

Según la investigación de (Jamal N. Al-Karaki) se enumeran a continuación los retos de enrutamiento:

- Despliegue del nodo.
- Consumo de energía sin perder precisión.
- Informes de datos del modelo.
- Nodo / Enlace Heterogeneidad.
- Tolerancia a fallos.
- Escalabilidad.
- Dinámica de Red.
- Medios de transmisión.
- Conectividad.
- Cobertura.
- Agregación de datos.
- Calidad de servicio.

2.1.10 Ventajas e inconvenientes de las redes de sensores.

Las ventajas de las redes de sensores especificadas por (López, 2013) son las siguientes:

- Movilidad y facilidad de reconfiguración
- Simplicidad y rapidez en la instalación
- Bajo consumo
- Escalabilidad.

Los inconvenientes:

- Caudal eficaz
- Capacidad de procesado y memoria
- Alcance
- Interferencia

2.1.11 Protocolos de enrutamiento en WSNs

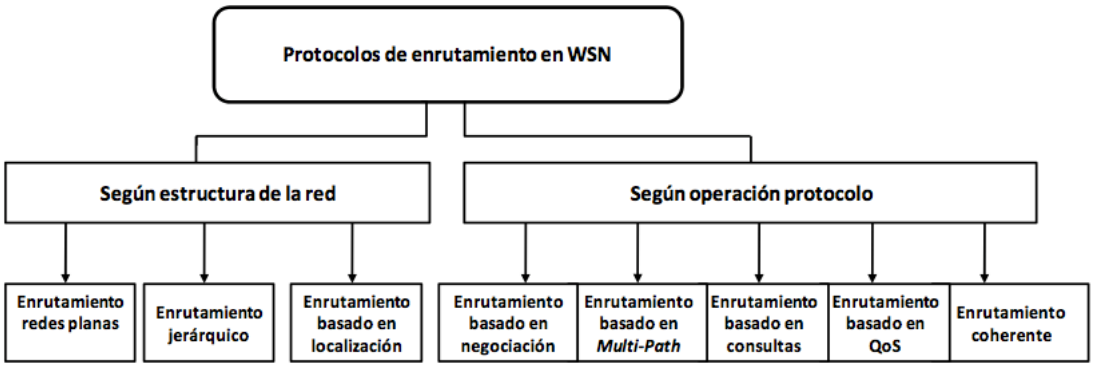


Figura 7. Taxonomía de los protocolos de enrutamiento en WSN

Fuente: (Hernández, 2010)

En las investigaciones llevadas a cabo por (Hernández, 2010) y (Jamal N. Al-Karaki) se explica que resulta primordial gestionar correctamente el consumo de los nodos sensores, para así equilibrar las prestaciones del sensor con su consumo. Uno de los factores que más influye en la limitación de consumo es el algoritmo de enrutamiento empleado. En los últimos años se han desarrollado multitud de técnicas para este propósito, proponiendo diversas alternativas sobre qué tipo de topología de red es la óptima para minimizar el consumo de energía y, en consecuencia, maximizar el tiempo de vida de la red.

De la mano de estas propuestas han aparecido multitud de protocolos, cada uno centrado en maximizar diferentes parámetros de la red. En la Figura 7 se propone una clasificación, a nivel de estructura de red y de operación del protocolo, que presenta una visión global de las diferentes técnicas de encaminamiento que existen en la actualidad.

Así mismo (Hernández, 2010) y (Jamal N. Al-Karaki) explican las técnicas de enrutamiento basándose en la forma de operar del protocolo, se distinguen cinco categorías:

1. Basados en Negociación (Negotiation Based), donde empleando una serie de mensajes de negociación se pretende eliminar duplicados en la información y prevenir que datos redundantes se envíen al siguiente nodo o al sumidero.
2. Basados en Multiruta (Multi-Path Based), donde se usan múltiples caminos en lugar de un único camino con el fin de mejorar el rendimiento.
3. Basados en Consultas (Query Based), donde los nodos destinatarios propagan la consulta de información (tarea de sensorización) desde un nodo hacia la red y cuando se encuentra un nodo que posee dicha información, éste responde a la consulta enviando los datos al que inició la consulta.
4. Basados en Calidad de Servicio (QoS Based), donde la red debe satisfacer ciertas métricas de QoS, como delay, energía, ancho de banda, cuando envía datos al nodo sink (sumidero), manteniendo de esta forma la red balanceada en cuanto a consumo de energía y calidad de la información.
5. Basados en Coherencia (Coherent Based), donde la información es enviada después de un mínimo procesado a los nodos encargados de la agregación. El procesamiento en coherencia es una estrategia típica para elaborar algoritmos de enrutamiento eficientemente energéticos.

Además (Hernández, 2010) y (Jamal N. Al-Karaki) explican que basándose en la estructura de la red, se tiene principalmente tres tipos de redes:

1. **Redes Planas (Flat Networks),** en las que todos los nodos desempeñan el mismo papel. En este tipo de redes la labor de sensorizar es realizada en colaboración.
2. **Redes Jerárquicas (Hierarchical Networks),** en las que existen nodos con distintos tipos de rol. Aquí se establecen diversos niveles en la red, en función del papel de los nodos.
3. **Encaminamiento basado en Localización (Location-based routing),** donde cada nodo dispone de un sistema que permite conocer la posición exacta del resto de nodos, y emplea esta información para la transmisión de datos.

2.1.12 Enfoques de Integración WSN-Redes TCP/IP

Según (Lucas Iacon, 2012), la integración WSN TCP/IP implica dos niveles a ser resueltos: Arquitectura y Protocolos de Interconexión.

2.1.12.1 Nivel de Arquitectura

Este nivel toma en cuenta cuál es el elemento WSN que tendrá dirección IP (real o virtual), y se resuelve utilizando dos enfoques: gateway y redes overlay.

- **Gateway.-** Este enfoque (Figura 8), se basa en que los nodos no cuentan con dirección IP, siendo la estación base la que tiene dirección IP y actúa como gateway de la capa de aplicación, traduciendo los protocolos de la capa inferior de ambas redes (TCP/IP y p. ej. ZigBee).

  El gateway es el único punto de acceso a la red, permite tomar los datos y comandos de cada WSN en el protocolo nativo (p. ej. ZigBee) y los convierte a

TCP/IP para luego, por intermedio de alguna red mayor (p.ej. Internet) presentarlos al cliente. Este enfoque permite trabajar con nodos sensores que cuenten con requerimientos escasos de cómputo, memoria y consumo de energía, ya que no requiere cargas extras de protocolo en los nodos sensores.

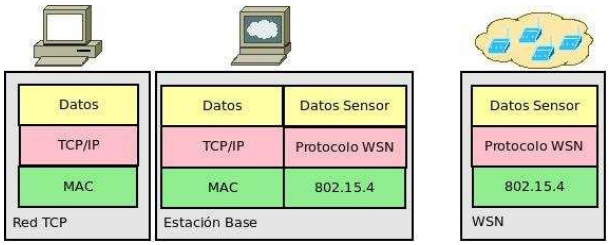


Figura 8. Enfoque de Gateway

Fuente: (Lucas Iacon, 2012)

- **Redes Overlay**.- Este enfoque de integración permite integrar redes con distintos protocolos mediante el solapamiento de uno de los protocolos sobre el otro. En el caso de la integración WSN - TCP/IP, se denomina TCP/IP "overlay" Sensor Networks, ya que se embebe parte o toda la pila TCP/IP en los nodos sensores (Figura 9).

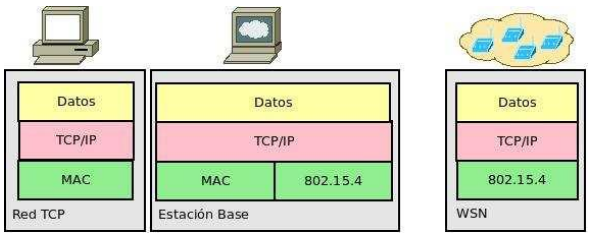


Figura III.- Enfoque de redes overlay. Adaptado de [19].

Figura 9. Enfoque de redes overlay

Fuente: (Lucas Iacon, 2012)

Estudios muestran que el enfoque Gateway consume menos procesamiento y recursos de energía que el enfoque overlay. (Lucas Iacono C. G., 2013)

2.1.12.2Nivel de Protocolos de Interconexión

En este apartado, se analizan los dos enfoques propuestos en el nivel de Protocolos de Interconexión para la integración WSN-TCP/IP: basados en estándares y ad-hoc.

- **Basados en estándares.-** En este enfoque, los protocolos basan la gestión de datos y comandos de las WSN en estándares como:

- Servicios Web.
- Lenguajes de descripción. Por ejemplo XML (Extensible Markup Languaje) [21].
- Estándares de sensores como IEEE 1451 [22] y SensorML [23].
- Protocolos Web tales como SNMP (Simple Network Management Protocol), HTTP, etc.

Estos lenguajes y protocolos si bien requieren mayores recursos de memoria y procesador en los nodos sensores, permiten estandarizar los datos prácticamente desde el momento en que son obtenidos por el nodo fuente.

- **Protocolos de interconexión ADHOC**

Este enfoque, tiene como principal ventaja el permitir desarrollar programas adaptados a las necesidades del usuario y de las aplicaciones. En la mayoría de los casos, esta técnica no necesita cargar funciones extras a los componentes de las WSN, los cuáles si se necesitan al momento de utilizar protocolos basados en estándares (XML, IEEE 1451, etc.). Luego, se puede optimizar el consumo de energía y de los recursos de hardware, ya que los nodos solo necesitan procesar el protocolo de la red de sensores, siendo la estación base, la encargada de implementar el protocolo ad-hoc.

2.2 Tipos de sensores aplicados en transporte y movilidad

A continuación se detallan algunos tipos de sensores:

2.2.1 Sensor facial de emociones

Es un dispositivo portátil que se utiliza para monitorizar las reacciones corporales y traducirlas en datos sobre emociones. El dispositivo recoge datos sobre la temperatura corporal, pulsaciones, presión arterial o conductividad eléctrica de la piel entre otros parámetros. Los sensores registran las variaciones de las medidas fisiológicas y los datos se suben a un servidor remoto para la conversión de esas medidas fisiológicas en estados emocionales.

Si es posible el mismo dispositivo convierte los datos fisiológicos en datos sobre emociones. Es decir, el mismo dispositivo utilizará las fórmulas adecuadas para interpretar los parámetros corporales. (Tuñón, 2014)

2.2.2 Autoemotive

Permite detectar y diagnosticar en tiempo real el estado de salud del conductor y notificarlo a los demás conductores. Se compone de varios dispositivos que capturan varias manifestaciones físicas de las emociones. El estrés de los conductores puede ser medido. Por otra parte también hemos demostrado que es posible capturar el ritmo cardíaco, la respiración y la variabilidad del ritmo cardíaco de forma remota con una cámara barata. (Hernandez, 2014)

2.2.3 Q Sensor

Mide la conductividad, temperatura y movimiento de la piel para registrar las reacciones de su portador a determinados eventos.

Este tipo de dispositivos toman medidas sobre el nivel de activación del sujeto (actividad electrodermal), fijándose en su sistema nervioso simpático (es decir, el que nos prepara para la acción). Este sistema se asocia con un estímulo emocional no neutro, por lo que tiene utilidad en la inferencia de algunos estados emocionales. (KelionBBC, 2014)

Explicado de una manera suscinta, una situación que tiene ligada una alta carga emocional (normalmente una situación asociada con el estrés o la tensión) hará que nuestras glándulas sudoríparas segreguen sales, con lo que aumentará la conductividad de nuestra piel. En caso opuesto, cuando el sujeto esté en calma, dicha conductividad disminuirá, lo que será muy útil como medida de posibles emociones negativas. (KelionBBC, 2014)

Figura 10. Q sensor: sensor afectivo.
Fuente: (KelionBBC, 2014)

2.2.4 Medición de estrés

Los biomarcadores más ampliamente utilizados de excitación emocional son:

2.2.4.1 Eye Tracking

Hasta la fecha, el seguimiento de los ojos es el único método en la investigación de la conducta humana que hacen posible medir de manera objetiva y cuantificar los movimientos del ojo en tiempo real.

Con la evolución de la tecnología informática, el seguimiento de los ojos se ha convertido en una herramienta no intrusiva, asequible y fácil de usar en la investigación

de la conducta humana que permite medir la atención visual, ya que objetivamente vigila dónde, cuándo, y lo que la gente mira. (Dalia Bagdziunaite, 2017)

2.2.4.2 Respuesta galvánica de la piel (GSR)

Es uno de los marcadores más sensibles para la activación emocional, también conocida como conductancia de la piel (SC) o actividad electro-dérmica (EDA). EDA modula la cantidad de secreción de sudor de las glándulas sudoríparas. La cantidad de glándulas sudoríparas varía a través del cuerpo humano, siendo más alta en las regiones de manos y pies (200-600 glándulas sudoríparas por cm2). Mientras que la secreción de sudor desempeña un papel importante para la termorregulación y la discriminación sensorial, los cambios en la conductancia de la piel en las regiones de la mano y del pie también se desencadenan muy impresionante por la estimulación emocional, a mayor excitación, mayor es la conductancia de la piel. Es digno de mención que ambos estímulos ("feliz" o "alegres") y negativos ("amenaza" o "triste") positivos pueden resultar en un aumento de la excitación y en un aumento de la conductancia de la piel.

La conductancia de la piel no está bajo control consciente. En su lugar, se modula de manera autónoma por la actividad simpática que impulsa el comportamiento humano, los estados cognitivos y emocionales en un nivel subconsciente. Por lo tanto, la conductancia de la piel ofrece una visión directa en la regulación emocional autónoma. Se puede utilizar como alternativa a los procedimientos de prueba de auto-reflexión, o mejor aún como fuente adicional de visión para validar auto-informes verbales o entrevistas de un encuestado. (Javier Martínez Fernández, 2012)

2.2.4.3 Electroencefalografía (EEG).

Electroencefalogramas (encéfalo = cerebro), o EEG, es la tecnología para la grabación de este ipo de electricidad a partir de la superficie del cuero cabelludo. El electroencefalograma registra la suma neta de todos los campos eléctricos generados por los sensores del cerebro (llamados electrodos) adheridos al cuero cabelludo. EEG es una técnica de grabación no invasiva y completamente pasiva. Cuenta con una excelente resolución temporal, es decir, puede tomar cientos a miles de instantáneas de la actividad eléctrica a través de múltiples sensores en un solo segundo. Esto hace que el EEG un candidato ideal para estudiar la evolución temporal precisa de procesamiento cognitivo y emocional. (Baltrusaitis, 2014)

2.2.5 Sensor Cutáneo

Este sensor que se puede llevar puesto, mide 20x20 milímetros y está fabricado con un polímero flexible y casi totalmente transparente. Aplicado sobre la piel, el senspr puede medir directamente cuándo, y con qué intensidad, se pone la "piel de gallina" ante determinadas situaciones que implican una respuesta emocional, tiene una alta estabilidad térmica.

El sensor utiliza **PEDOT: PSS**, un material flexible si se compara a los frágiles metales de los materiales conductores estándar. Los capacitores se embebieron en un sustrato de silicona a través de un proceso de revestimiento en múltiples pasos, lo que les dio su forma espiral y su estructura. El resultado fue un sensor de alta capacidad y elasticidad, pero con un grosor de apenas 1,2 micras. (KelionBBC, 2014)

2.2.6 Pantalla led informativa y parlante de exceso de velocidad

La pantalla LED informativa y el parlante sirven para informar a los pasajeros en caso de que el conductor exceda la velocidad permitida, en la pantalla se verá la velocidad a la que conduce y en caso de sobrepasarla se emitirá una luz intermitente con una señal y los parlantes permitirán emitir una alarma sonora para alertar a los pasajeros y al conductor**.** (Agencia Nacional de Regulación y Control del Transporte Terrestre, 2015)

2.2.7 Cámaras de video infrarrojas

Las cámaras de video infrarrojas permiten obtener video en tiempo real del interior del vehículo, sobre todo el estado del conductor. (Agencia Nacional de Regulación y Control del Transporte Terrestre, 2015)

2.2.8 GPS

El GPS permite obtener las coordenadas de ubicación exactas del vehículo. (Agencia Nacional de Regulación y Control del Transporte Terrestre, 2015)

2.2.9 Botones de auxilio

Permiten obtener una señal de auxilio en la central de control de los vehículos. (Agencia Nacional de Regulación y Control del Transporte Terrestre, 2015)

2.2.10 Módulo de conexión satelital

Canal de comunicación para el envío de la información a servidores digitales. (Agencia Nacional de Regulación y Control del Transporte Terrestre, 2015)

2.2.11 Sensor en el volante

Cuenta cuántas veces por minuto el conductor realiza pequeñas correcciones en la dirección. Esta advertencia puede ser variable, lo normal es un cartel en la pantalla digital del cuadro de instrumentos y una alarma sonora (por ejemplo un pitido) pero también puede ser incluso una vibración en el volante. (Ibañez, 2011)

2.2.12 Detector de somnolencia-interruptor de mercurio

Un interruptor de mercurio es un dispositivo cuyo propósito es permitir o interrumpir el flujo de corriente eléctrica en un circuito eléctrico, dependiendo de su alineamiento relativo con una posición horizontal. (Franklin Silvio Córdova Ochoa, 2012)

Los interruptores de mercurio consisten en uno o más conjuntos de contactos eléctricos en una ampolla de cristal sellado que contiene cierta cantidad de mercurio. El cristal sellado puede contener aire o gas inerte. La gravedad está constantemente desplazando la gota de mercurio al punto más bajo.

Figura 11. Sensor de mercurio.
Fuente: (Franklin Silvio Córdova Ochoa, 2012)

2.2.13 Cámara de video

Capta información del rostro del conductor, la cual será analizada para determinar las emociones. La cámara puede ser de tipo IP, “una cámara IP o cámara de video de internet, es un dispositivo que capta y trasmite una señal de audio/video través de una red IP estándar u otro dispositivo de red”.

Básicamente una cámara IP se compone de un lente, un sensor de imagenes, un procesador de imágenes, un chip de compresión de video y un chip Ethernet que ofrece conectividad de red para la transmisión de datos. (Novillo, 2014)

2.2.14 Sensor de temperatura

Los sensores de temperatura permiten monitorear el estado de una persona, una temperatra baja o excesiva de los valores de temperatura normales tienen una afectación en el comportamiento. (Durán, 2015)

2.2.15 Sensor de frecuencia cardíaca

El pulso es el latido de una arteria que se siente sobre una saliente ósea. Cuando se contrae el ventrículo izquierdo, la sangre pasa a través de las arterias y venas de todo el cuerpo. Esta onda de sangre es el pulso. El sensor permite determinar la frecuencia cardíaca a través de la medición del pulso. (Durán, 2015)

2.2.16 Sensor de presión sanguínea /presión arterial

La presión sanguínea es la presión de la sangre contra las parees arteriales. La presión sistólica es el punto de presión más alto sobre las paredes arteriales que coincide con la contracción de los ventrículos y empuja la sangre a través de las arterias al inicio de la sístole. Cuando el corazón reposa entre latidos durante la diástole, la presión sanguínea cae. (Durán, 2015)

2.2.17 Sensores biomédicos

Los sensores biomédicos transforman procesos biológicos en señales eléctricas u ópticas.

2.3 Mecanismos y dispositivos utilizados para la extracción de emociones

2.3.1 Voz

En estos mecanismos se tienen en cuenta las características de la voz; normalmente extrayéndose las emociones por medio de comparaciones con grabaciones previamente hechas, por ejemplo el software EmoSpeech. (Rey, 2012)

2.3.2 Imagen

Para el análisis de la imagen, se usa una cámara para la extracción de los valores RGB (cantidad de rojo, verde y azul presente en cada píxel de la imagen). Aunque no tienen una representación directa con las emociones, se explican algunos parámetros típicos de las imágenes, cuyo conjunto dará lugar a dicha inferencia: resolución, tono, brillo, contraste. (Rey, 2012)

En cuanto a los dispositivos usados para la extracción de emociones, típicamente se usarán siempre cámaras en lugar de algún otro tipo de sensores; puede ser la plataforma *Kinect, que es OpenNI,* un entorno muy robusto y útil para aplicaciones muy heterogénea. (Rey, 2012)

2.3.3 Plataforma Emotient

La plataforma emotient usa expresiones faciales para entender las reacciones emocionales, se considera un método de investigación no intrusiva, únicamente se

requiere un video de la cara grabada para analizar, agregar y exportar todos los datos en bruto y métricas. (EMOTIENT, 2017)

Emotions carga por lotes todos los vídeos y rápidamente extrae todos los datos de la expresión facial, analiza, y exporta los resultados directamente. Además permite ahorrar tiempo y recursos ya que tiene unidades de actuación que extraen automáticamente, y pasan directamente a analizar los datos en lugar de recogerlos. (EMOTIENT, 2017)

Figura 12. Plataforma web imotions- Combina con Stimuli, Eye Tracking, EGG, GSR.
Fuente: (EMOTIENT, 2017)

Es posible emplear la plataforma imotions para determinar el resultado del reconocimiento facial. El video se envìa a la nube para su análisis y determinación de las emociones, lo cual se retorna al vehículo para producir una acción que permita la reacción del conductor.

2.4 Cloud Computing

2.4.1 Definición

El NIST National Institute of Standars and Technology define la computación en la nube como: “Un modelo que permite el acceso bajo demanda a través de la red a un conjunto compartido de recursos de computación configurables (p.e. redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar rápidamente con el mínimo esfuerzo de gestión o interacción del proveedor de servicios” (Peter Mell, 2011)

Cloud Computing agrupa las tecnologías, servicios y aplicaciones que son similares a las de internet y las convierte en utilidades de autoservicio. El uso de la palabra “**cloud**” según (Luis, 2012) se refiere a dos conceptos esenciales:

- **Abstracción**. La computación en la nube abstrae los detalles de la implementación del sistema de los usuarios y desarrolladores. Las aplicaciones se ejecutan en sistemas físicos que no están especificados, los datos se almacenan en posiciones que son desconocidas, la administración de sistemas está externalizada a otros y el acceso por parte de los usuarios es ubicuo (desde cualquier lugar, en cualquier disposiivo y en cualquier momento).
- **Virtualización**. La computación en nube virtualiza sistemas agrupando y compartiendo recursos. Los sistemas y el almacenamiento son provistos a medida que se requieren desde una infraestructura centralizada; los costes se evalúan con indicadores y métricas previamente establecidas, la multitenancy (multitenencia, multialquiler) está habilitada y los recursos son escalables de un modo muy ágil.

Entre las ventajas más importantes de la virtualización (Luis, 2012) se puede mencionar:

- Reduccion de los costos de espacio y consumo.

- Rapida incorporacion de nuevos recursos para los servidores virtualizados.
- Administracion global centralizada y simplificada.
- Facilidad para la creacion de entornos de test que permiten poner en marcha nuevas aplicaciones sin detener el desarrollo, agilizando el proceso de las pruebas.
- Aislamiento: un fallo en una maquina virtual no afecta al resto de maquinas virtuales.

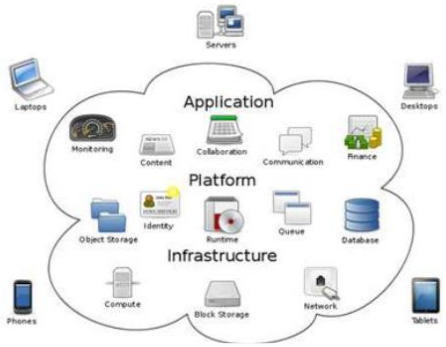


Figura 13. VIsión de Cloud Computing.
Fuente: (Sajjad Hussain Shah, 2013)

2.4.2 Características esenciales de cloud computing

La Figura 14 muestra el modelo de trabajo completo de la definición NIST con la indicación de las diferentes categorías de modelos (servicio y despliegue), sus características fundamentales (autoservicio bajo demanda, acceso universal de banda ancha, compartición de recursos-pooling, elasticidad inmediata, servicio medido) y comunes (escala masiva, homogeneidad, virtualización, software de bajo coste, computación flexible, distribución geográfica, orientación a servicios, seguridad avanzada). (Luis, 2012)

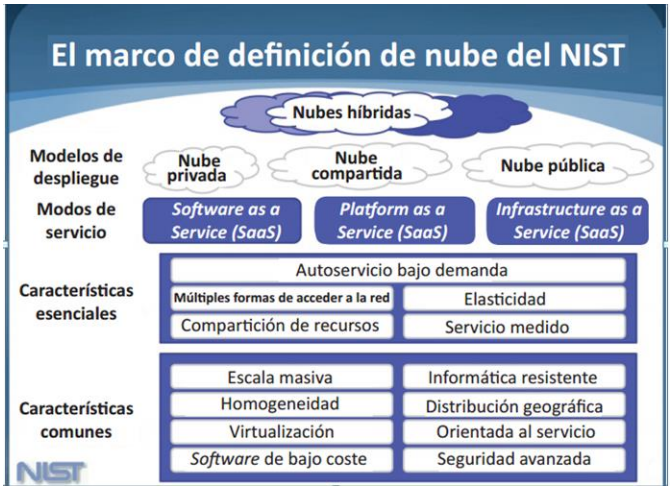


Figura 14. Marco de definición de nube del NIST.

Fuente: (Sajjad Hussain Shah, 2013)

Según el NIST, el modelo (Figura 14) tiene las siguientes características:

- **Autoservicio bajo demanda.** Un consumidor puede proveerse unilateralmente de características tales como tiempo de servidor y almacenamiento en red, a medida que lo necesite sin requerir interacción humana con el proveedor del servicio. (ORSI)

- **Acceso ubicuo a la Red.** Los recursos son accesibles a través de la red por medio de mecanismos estándar que son utilizados por una amplia variedad de dispositivos de usuario, desde teléfonos móviles hasta ordenadores portátiles o PDA (Personal Digital Assistant). (p.e. teléfonos móviles, computadoras portátiles, laptops, PDA's, tabletas, ultrabooks. (ORSI)

- **Agrupación de recursos independientes de la posición.** Los recursos de computación del proveedor son agrupados (pooled) para servir a múltiples consumidores utilizando un modelo multi-distribuido (multitenant), con diferentes

recursos físicos y virtuales asignados y reasignados dinámicamente conforme a la demanda del consumidor. Existe una sensación de independencia de la posición exacta de los recursos proporcionados pero se puede ser capaz de especificar la posición a un nivel más alto de abstracción (por ejemplo, país, región geográfica o centro de datos). Ejemplos de recursos incluyen almacenamiento, procesamiento, memoria, ancho de banda de la red y máquinas virtuales. (Microsoft, 2012)

- Los recursos (almacenamiento, memoria, ancho de banda, capacidad de procesamiento, máquinas virtuales, etc.) de los proveedores son compartidos por múltiples usuarios a los que se van asignando capacidades en forma dinámica según sus peticiones. Los usuarios pueden ignorar el origen y la ubicación de los recursos a l**o**s que acceden, o es posible que sea conscientes de su situación a determinado nivel, como el de CPD (Centro de procesamento de datos) o el de país. (Microsoft, 2012)

- **Elasticidad rápida**. Las funcionalidades se pueden proporcionar en forma rápida y elástica, en algunos casos automáticamente de modo que se puede escalar rápida y fácilmente. Normalmente, sus características disponibles de **aprovisionamiento** dan la sensación al consumidor de ser ilimitadas y pueden ser adquiridas en cualquier cantidad y en cualquier momento. (Microsoft, 2012)

- **Servicio medido.** Los sistemas de computación en la nube controlan y optimizan el uso de recursos automáticamente potenciando la capacidad de medición en un nivel de abstracción apropiado al tipo de servicio (almacenamiento, procesamiento, ancho de banda y cuentas activas de

usuario). El uso de recursos se puede monitorizar, controlar e informar, lo que proporciona transparencia tanto al proveedor como al consumidor de los servicios. (Microsoft, 2012)

- **Costes más bajos.** Se producen considerables reducciones de costes cuando se compara con los altos grados de eficiencia y de buena utilización que producen los modelos y herramientas de la nube con otros productos similares del mercado. (Microsoft, 2012)

- **Facilidad de utilización**. Dependiendo del tipo de servicio que contrate normalmente no se requerirán licencias de hardware ni de software para implementar el servicio. Por otra parte los productos se ofrecen adaptados al usuario normal, requiriendo a lo sumo pequeños cursos de formación. (Microsoft, 2012)

- **Calidad de Servicio (QoS).** La calidad del servicio se obtiene por lo general mediante contrato de su proveedor. (ORSI)

- **Fiabilidad.** La potencia y escalamiento de las redes de computación de los proveedores garantizan la fiabilidad de los servicios ofertados, en la mayoría de los casos, con un nivel de fiabilidad tan alto o más que los proveedores clásicos más respetados (que por otra parte están migrando sus servicios también a la nube como en el caso de Oracle, SAP, IBM…). (ORSI)

- **Administración externalizada de TI.** Un despliegue de cloud computing permite la gestión de la infraestructura de computación mientas se gestionan,

en paralelo, sus negocios. En la mayoría de los casos este modelo de externalización (outsourcing) de TI consigue considerables reducciones de costes tanto de equipos como de recursos humanos. (Computing, 2010)

- **Simplificación de la actualización y mantenimiento**. Dado que el sistema es centralizado (aunque técnicamente actúa como descentralizado y distribuido) se pueden aplicar fácilmente, parches y actualizaciones de software (upgrades). (Computing, 2010)

- **Facilidad para superar barreras**. El cloud computing rompe barreras físicas y virtuales, de modo que es ideal para jóvenes emprendedores y empresas start-up además de grandes empresas, por facilidad de uso para su adaptación tecnológica. (ORSI)

2.4.3 Modelos de la nube

En (Luis, 2012), se clasifica la computación en la nube en dos conjuntos distintos de modelos:

2.4.3.1 Modelos de despliegue.

Se refieren a la posición (Localización) y administración (gestión) de la infraestructura de la nube (Pública, Privada, Comunitaria, Híbrida).

2.4.3.2 Modelos de servicio.

Se refieren a los tipos específicos de servicios a los que se puede acceder en una plataforma de cloud computing (Software como Servicio, Plataforma como Servicio e Infraestructura como Servicio).

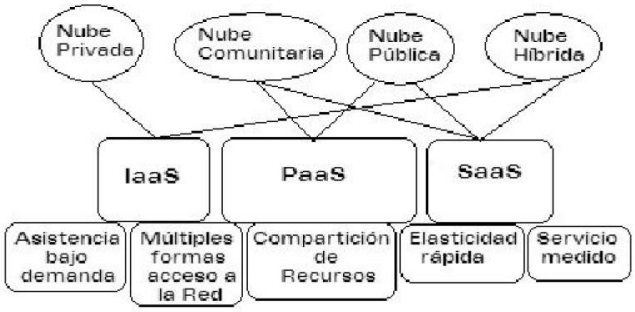


Figura 15. Modelos de despliegue y servicios de la Nube.

Fuente: (Luis, 2012)

A continuación en la Figura 16 se muestran los servicios de Cloud Computing por capas. Los servicios de sistemas operativos pueden ser ofrecidos como PaaS e IaaS, y los lenguajes de programación como Paas y SaaS. (Bocchio, 2014)

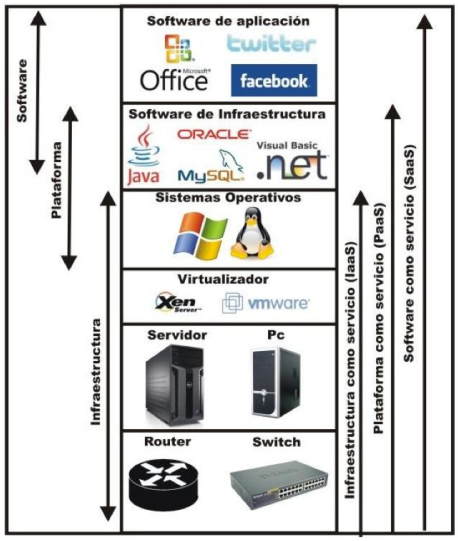


Figura 16. Servicios de Cloud Computing por capas.

Fuente: (Bocchio, 2014)

- **Software como Servicio (SaaS).**

En este servicio los usuarios no tienen que manejar máquinas virtuales ni plataformas de software que hospedan la aplicación, simplemente es una alternativa para correr distintas aplicaciones desde Internet como si estuviesen en sus equipos de cómputo. El usuario carece de cualquier control sobre la infraestructura o sobre las propias aplicaciones, a excepción de las posibles configuraciones de usuario o personalizaciones que se le permitan. (Luis, 2012)

En un modelo SaaS las aplicaciones se descargan de la nube y se ejecutan directamente a cambio de una cuota que puede ser una cantidad determinada o gratuita. Ejemplos de proveedores son: Google Apps, Zoho, Salesforce.com, Dropbox, GlideOS, Wuals, Evemote, Office 365. El modelo SaaS es un modelo de software basado en la Web que proporciona al software totalmente disponible a través de un navegador web. Las aplicaciones son accesibles desde diferentes dispositivos cliente a través de una interfaz cliente ligera tal como un navegador. (ORSI)

En un modelo SaaS el usuario no tiene que preocuparse por conocer donde está alojado el software, qué tipo de sistema operativo se utiliza o si está escrito en lenguaje PHP, Java o .Net. Además, el usuario no tiene que instalar ningún programa de software como si se hace en el modelo tradicional. El consumidor no gestiona ni controla la infraestructura fundamental de la nube, incluyendo red, sistemas operativos, servidores ni incluso las características. (ORSI)

Este modelo ofrece espacio de almacenamiento, capacidad de proceso, servidores y otro equipamiento físico, en pago por uso. Puede también incluir la entrega de sistemas operativos y tecnologías de virtualización para gestionar los recursos. El cliente SaaS

“alquila” (pago por uso y prestaciones) recursos informáticos en lugar de comprarlos e instalarlos en su propio centro de datos. (ORSI)

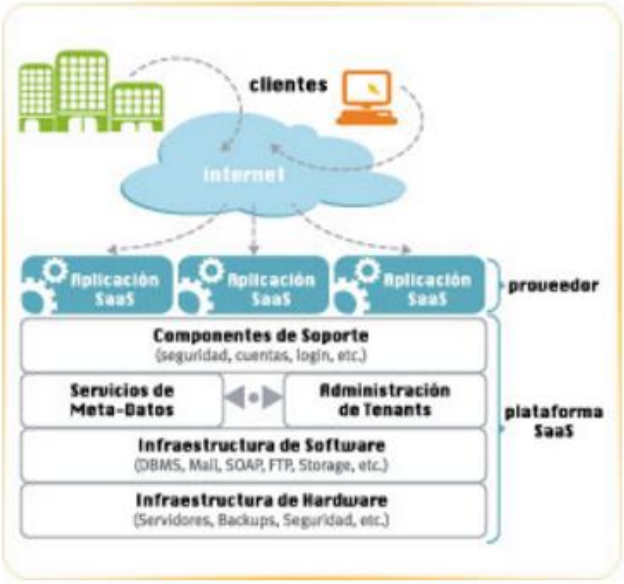


Figura 17. Arquitectura SaaS.

Fuente: (ORSI)

Software como servicio (SaaS) es el servicio de más alto nivel, ofrece aplicaciones para el usuario final. Según la definición del NIST, SaaS es el servicio que permite al usuario utilizar aplicaciones que están corriendo en una infraestructura cloud. Estas aplicaciones son accesibles desde diferentes dispositivos a través de un browser. El consumidor de este servicio no administra ni tiene control sobre la infraestructura cloud subyacente, como son la red, los servidores, sistemas operativos, almacenamiento, ni siquiera sobre las características técnicas de la aplicación.

Los requisitos técnicos de las aplicaciones SaaS pueden implementarse a través de técnicas modernas de diseño y programación: OOP (Programación Orientada a Objetos), SOA (Arquitectura Orientada a Servicios). (ORSI)

- **Plataforma como servicio (PaaS).**

En este servicio, está instalada una plataforma de software para hospedaje de aplicaciones que serán ofrecidas a los usuarios. En esta plataforma los usuarios no manejan máquinas virtuales. (Bocchio, 2014)

Al usuario se le permite desplegar aplicaciones propias (ya sean adquiridas o desarrolladas por el propio usuario) en la infraestructura cloud de su proveedor, que es quien ofrece la plataforma de desarrollo y las herramientas de programación. En este caso, es el usuario quien mantiene el control de la aplicación, aunque no de toda la infraestructura subyacente. (Luis, 2012)

Esta plataforma proporciona a los desarrolladores un despliegue rápido. Ejemplos de proveedores son: Google App Engine, Salesforce.com, Microsoft, Azure. (Sajjad Hussain Shah, 2013)

- **Infraestructura como servicio (IaaS).**

Según (Bocchio, 2014) este servicio se ofrece como hardware, los proveedores de la infraestructura física gestionan los recursos de almacenamiento, memoria y procesamiento a través de máquinas virtuales, para que los usuarios los utilicen de la forma como ellos decidan.

El proveedor ofrece al usuario recursos como capacidad de procesamiento, de almacenamiento o comunicaciones, que el usuario puede utilizar para ejecutar cualquier tipo de software, desde sistemas operativos hasta aplicaciones**.**

Infraestructura compartida como redes, servidores y almacenamiento. Ejemplos de proveedores son: Amazon AWS, Dell, Arsys, Strato.

Por último, según el NIST (Peter Mell, 2011) hay cuatro posibles formas de desplegar y operar una infraestructura de Cloud Computing:

- **Nube privada.**

Los servicios cloud no son ofrecidos al público en general. La infraestructura es íntegramente gestionada por una organización. La infraestructura de esta nube está operada únicamente por una organización, Puede ser administrada por la organización o por un tercero y puede existir dentro de la misma (on premises) o fuera de la misma (off premises) (NIST 2009). La nube privada se carácteriza porque es propiedad de la empresa que la utiliza y por consiguiente, está bajo su control, y en consecuencia decide quien debe tener acceso a la nube. En la práctica significa que el centro de datos de la nube (normalmente virtualizado) está localizado dentro del perímetro de seguridad (cortafuegos, firewall) de la empresa.

En general, en un modelo de funcionamiento de nube privada, la gestión de la seguridad y las operaciones diarias de los servicios alojados (host) son responsabilidad del departamento interno de TI de la organización, o de una empresa externa que se ha subcontratado con un acuerdo contractural SLA. En consecuencia, en este modelo de gobierno directo, un cliente de una nube privada debe tener un alto grado de control sobre los aspectos físicos y lógicos de la seguridad de la infraestructura de la nube y en consecuencia será más fácil para el cliente cumplir con los estándares, políticas y regulación de la seguridad.

- **Nube pública**.

La infraestructura es operada por un proveedor que ofrece servicios al público en general. La nube pública es el modelo estándar de la computación en la nube, en el cual un proveedor de servicios pone sus recursos tales como aplicaciones y

almacenamiento disponibles al público en general a través de internet por medio de aplicaciones o servicios web. Los servicios de la nube pueden ser libres (gratuitos) o bien ofertados mediante un modelo de pago por uso.

Normalmente, la nube se opera y gestiona en un centro de datos propiedad del proveedor de servicios, que aloja múltiples clientes y utiliza aprovisionamiento dinámico. La implementación de una plataforma escalable de servicios y de pago por uso es también un elemento de interés para la elección de la nube pública.

Desde el punto de vista económico, utilizando una nube pública (también conocida como nube externa) puede ahorrar costes económicos de modo inmediato a una organización.

En una nube pública, la gestión de la seguridad y las operaciones es controlada por un proveedor que es responsable de la oferta de servicios de la nube. Por estas razones se tiene un control muy bajo de la seguridad física y lógica, al contrario de lo que sucede en una nube privada.

Ejemplos de proveedor de despliegue en la nube pública incluyen soluciones como Amazon Web Services, Google App Engine, Salesforce.com y Microsoft Azure.

- **Nube híbrida**.

Es la composición de dos o más nubes, por ejemplo, privada y pública, que permanecen como entidades únicas pero que coexisten por tener tecnologías que permiten compartir datos o aplicaciones entre las mismas (NIST). Este modelo pretende aprovechar las mejores características de los modelos públicos y privados, en una mezcla de ambos modelos.

Un ejemplo de un despliegue de nube híbrida puede ser el de una organización que despliega aplicaciones de software no críticas en la nube pública, mientas que las aplicaciones críticas o sensibles (apps) están en una nube privada, en la organización (on the premises). Las nubes híbridas combinan modelos de nube pública y privada y pueden ser especialmente efectivas con tipos de nube localizadas en la misma instalación.

Las nubes híbridas son nubes privadas que pueden tener también acceso a recursos externos, cortafuegos (firewall) durante perìodos de máxima demanda. Las nubes híbridas mantienen almacenamiento de datos “en casa” y alquilan anchos de banda con un modelo de pago a medida.

Un entorno de nube privada consta de múltiples proveedores internos y/o externos y es un despliegue posible para organizaciones. Con una nube híbrida las organizaciones pueden ejecutar aplicaciones no fundamentales (non-core) en una nube pública, mientras mantienen las aplicaciones fundamentales y los datos sensibles internos en una nube privada.

- **Nube comunitaria**.

Una nube comunitaria (community) es aquella nube que ha sido organizada para servir a una función o propósito común. Puede ser para una organización o varias organizaciones, pero que comparten objetivos comunes como su misión, políticas, seguridad o necesidades de cumplimientos regulatorios (compliances). (Peter Mell, 2011)

Dentro de cada uno de los tres modelos, existen diferentes modelos de despliegue; por ejemplo, el modelo de entrega SaaS puede ser presentado a los usuarios en uno de los diferentes tipos de despliegue, tal como nubes privada, pública o híbrida. (Luis, 2012)

Existen distintos proveedores que ofrecen los servicios del Cloud Computing, en la Figura 18 se muestran ordenados los proveedores de acuerdo a los servicios que ofrecen hoy en día. (Pérez, 2012)

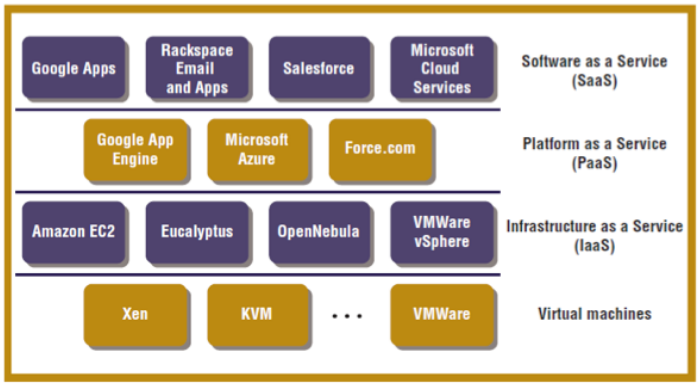


Figura 18. Servicios de Cloud Computing con proveedores.

Fuente: (Pérez, 2012)

2.4.4 Ventajas de cloud computing

Los autores (Luis, 2012), (ORSI) y (Lucas Iacono C. G., 2013) mencionan las siguientes ventajas:

1. El modelo genera grandes economías de escala que pueden ser trasladadas a los usuarios, transformando así de fijos en variables los costes en sistemas de información y poniendo, por tanto, las prestaciones de los sistemas más costosos al alcance de organizaciones de cualquier tamaño o de limitada capacidad inversora. Se elimina por tanto la necesidad de grandes inversiones y costes fijos en tecnologías de la información (TI) en utilities, que ponen al alcance de los usuarios la capacidad de computación: bajo

demanda, sin preocuparse de cómo o donde es generada y de modo flexible e instantánea.

2. Escalabilidad de los recursos.- A través de la escalabilidad, Cloud Computing puede resolver problemas de cómputo y almacenamiento de las aplicaciones.
3. Los usuarios pueden acceder fácilmente a los modelos de desarrollo de aplicaciones que utilizan servicios en la nube a fin de permitir la escalabilidad de los recursos.
4. Disminución del tiempo de implantación de nuevos servicios.
5. Capacidad de recuperación ante fallos.
6. Mayor resistencia a desastres.

Además según (Saha, Secure Sensor Data Management Model in a Sensor Cloud Integration Environment, 2015), la plataforma de cloud computing permite:

- El acceso a los recursos de TI.
- Compartir infraestructura común.
- Proporcionar servicios a través de aplicaciones web.
- Suministrar y liberar recursos y servicios en función de la demanda.
- La utilización simplificada de aplicaciones de recursos, almacenamiento de datos, intercambio de recursos y acceso a la red desde cualquier dispositivo conectado a Internet.
- La **utilización de recursos escalables** que ofrece cloud computing podría escalar rápidamente hacia arriba o hacia abajo de la escala de asignación de los recursos para satisfacer la demanda de la aplicación.

- **La gestión de recursos en tiempo de ejecución** (run-time) es otra de las ventajas de la computación en la nube. Esto facilita que los recursos defectuosos sean puestos en libertad rápidamente y nuevos recursos sean asignados. Cloud computing exhibe su característica de tolerancia a fallos automáticamente los recursos alternativos desovados (spawning-soltados o liberados) en caso de recurso defectuoso.
- **La utilización de recursos automáticos y eficientes y** gestión de los recursos satisfacen la plena utilización de uso de recursos. Incluso se permite la personalización y la asignación de recursos bajo demanda. Esto mejora el equilibrio de carga dinámico y por lo tanto mejora el rendimiento.
- **La computación en la nube ofrece espacio de almacenamiento casi ilimitado** sobre la base de pago. Esta característica elimina la crisis de espacio de almacenamiento de contenido de datos.
- **Un sistema de nubes se puede implementar en un corto período de tiempo**. La integración de software, incluso se produce de forma automática. La personalización local de este servicio se puede hacer con facilidad y un esfuerzo mínimo.
- Los servicios de computación en la nube **se pueden acceder en cualquier lugar mediante cualquier dispositivo** habilitado para Internet, como PC, tableta, móvil, ordenador portátil. No hay limitación de medio o lugar.
- La tecnología cloud computing puede proporcionar pleno apoyo a las aplicaciones basadas en WSN. **Cloud Computing puede calcular, almacenar, procesar y entregar los datos a la aplicación correcta.** Por lo tanto, desarrollar una potente aplicación sensor, la red de sensores integrada con la computación en la nube puede ser utilizada de manera eficiente.

- Ahorro, tanto en licencias como en la administracion del servicio y en los equipos necesarios.
- Implementacion rapida y baja en riesgos.
- Actualizaciones automaticas: No afectan negativamente a los recursos de TI.
- Portabilidad de información.
- Por otra parte, el modelo de la nube es más amigable con el medio ambiente; ahorro global de energía.
- El beneficio se extiende tambien a los consumidores, en el caso de videos y juegos los costos se reducen al pagar solo lo que se usa por el tiempo solicitado.

2.4.5 Desventajas de cloud computing

A continuación se explican algunas desventajas según (Luis, 2012):

- Pérdida de control por parte de los usuarios tanto sobre las aplicaciones y servicios como sobre los datos, en ocasiones muy sensibles, que se suben a nubes, con los consiguientes riesgos relativos tanto a privacidad como a la integridad de los mismos.
- Confiabilidad de los servicios ofrecidos, por ejemplo por google.
- Fuga de información (seguridad)
- Disponibilidad de las aplicaciones.
- Escalabilidad a largo plazo.

2.4.6 Arquitectura genérica para cloud computing

Figura 19. Capas básicas de Cloud Computing.
Fuente: (Adriana Cornejo, 2015)

En la investigación de (Adriana Cornejo, 2015) se explica que la arquitectura genérica para Cloud Computing está formada por las siguientes capas de abajo hacia arriba:

 Recursos físicos: Esta capa está compuesta por elementos físicos como servidores, almacenamiento y red, es decir, todo el hardware que interviene en la nube. Estos elementos pueden ser:

- **CPU, discos duros, memorias:** Estos elementos se encargan del procesamiento de la información, por lo que representan la parte más importante de Cloud Computing.
- **Redes:** Son los elementos de red que se encargan del transporte hacia los medios de almacenamiento.
- **Equipos de Enfriamiento:** Se encargan de mantener los elementos que intervienen en la nube, a una temperatura considerable, para evitar fallas o recalentamiento por uso.
- **Redundancia:** Aquí intervienen los respaldos y recuperación ante desastres, o por fallas como cortes de luz, caídas de servidores o sobrecarga de datos.

 Virtualización: Esta capa se encarga de la infraestructura virtual como un servicio, aquí están los virtualizadores que ayudan con la emulación de los recursos físicos.

 Infraestructura: Esta capa es la encargada de administrar el software de plataforma como servicio, como puede ser en el caso de la aplicación Openstack, Cloudstack.12

 Plataforma: En esta capa están los componentes de aplicación como servicio, aquí estarían los módulos o componentes en donde se despliegan las aplicaciones, por ejemplo en el caso de Openstack, Keystone, que es el módulo de autenticación, Dashboard que es la interfaz de usuario, también conocido como Horizon.

 Aplicación: En esta capa se incluyen los servicios basados en web y software como servicio.

2.4.7 Estudio comparado de las arquitecturas cloud computing.

TABLA 3. MATRIZ COMPARATIVA DE ARQUITECTURAS CLOUD COMPUTING.

Plataforma → Característica ↓	Amazon EC2	Microsoft Windows Azure	Google App Engine	Red Hat OpenShift	IBM SmartCloud	VMWare VCloud Suite	OpenStack
Escalabilidad automática (auto scaling)	Sí, a través de Amazon CloudWatch	Autoscaling application block y Windows Azure Fabric Controller.	BigTable y GFS	OpenShift HA Proxy	IBM SmartCloud Application Workload Service	VCloud Director	OpenStack Heat
Blueprints / Imágenes para acelerar el aprovisionamiento	Sí (AMI) – Imagen de máquina Amazon	Sí, provistas en una galería, y también imágenes propias guardadas	No	Sí (Single and Multitier VM Applications)	Sí	Sí, imágenes propias guardadas de máquinas virtuales VMWare	Sí, imágenes creadas por OpenStack y también compartidas por usuarios de la plataforma.
Soporta Sistema operativo Windows	• Windows Server® 2003 R2 • Windows Server 2008 • Windows Server 2008 R2 • Windows Server 2012	Sí • Windows Server 2012 Datacenter • Windows Server 2008 R2 SP1	No	No	• Sí • Microsoft Windows Server 2003 • Microsoft Windows Server 2008	Sí, todas las distribuciones virtualizables	Sí, Windows Server 2008 R2
Soporta Sistema operativo Linux	• Sí: • SUSE Linux Enterprise Server • Red Hat Enterprise Linux	• openSUSE 12.3 • SUSE Linux Enterprise Server 11 Service Pack 2 • Ubuntu Server 12.04 LTS • Ubuntu Server 12.10 • Ubuntu Server 13.04 • OpenLogic CentOS 6.3 • Ubuntu Server 12.10 DAILY	Sí, pero las aplicaciones corren en un sandbox y Google provee acceso limitado al sistema operativo, el cual no puede ser alterado.	Sí, Red Hat Linux Enterprise	Sí Red Hat Enterprise Linux SUSE Linux Enterprise Server	Sí, todas las distribuciones virtualizables	• Debian GNU/Linux wheezy • Fedora / Red Hat Enterprise Linux / CentOS / Scientific Linux • openSUSE / SLES11 SP2 • Ubuntu 12.04 LTS (Precise Pangolin)
Soporte para lenguajes	• C++ • C# • Java • Perl • Python • Ruby	• .Net • Java • Node.js • Python	• Python • Java • Go(experimental)	• Java • Ruby • node.js • Python • PHP • Perl	• Java • PHP	• Java • C# • C++	APIs Para: • PHP • Python • Java • C#/.NET • Ruby
Soporte para almacenamiento de datos	• Amazon SSS • Amazon Relational DB Service • Amazon SimpleDB • SQL Server® Express • SQL Web • SQL Server Standard	• SQL Relacional • Almacenes de tablas NoSQL • Blob no estructurado	• Base de datos no relacional "BigTable". • No soporta bases de datos relacionales.	• MySQL • PostgresSQL • Mongo DB • SQLite	• DB2 • Oracle • MS SQL • MySQL • Informix • Sybase	• Oracle • SQL Server • VMware vFabric • Postgres • Múltiples distribuciones de Hadoop	• Object Storage (Swift) • Block Storage (Cinder) • MySQL hosts DB for Nova, Glance, Cinder, and Keystone
Soporte para Colas	Amazon Simple Queue Service	Windows Azure Service Bus, Colas FIFO con protocolos Rest, AMQP, WS	App Engine Task Queue	IronMQ	WebSphere Message Broker V8.0	RabbitMQ Protocolos AMQP, MQTT and STOMP	Rabbit MQ Server, AMPQ

TABLA 3. MATRIZ COMPARATIVA DE ARQUITECTURAS CLOUD COMPUTING.

Plataforma → Característica ↓	Amazon EC2	Microsoft Windows Azure	Google App Engine	Red Hat OpenShift	IBM SmartCloud	VMWare VCloud Suite	OpenStack
Servidor Web	• Apache • IIS • Otros	IIS V7.5	Jetty Web Server	Apache	WebSphere Application Server V7.0 and V8.0	• Apache • IIS • Otros	Ofrece IaaS, no PaaS
Alternativas de hipervisores	XEN y LXC (Linux Containers)	Windows Azure Hipervisor (customized Hyper-V)	XEN/KVM	• KVM (Kernel-based VM) • Xen • QEmu	• VMWare • Hyper-V • Otros	VMWare	• XenServer/XCP • KVM • QEMU • LXC • ESXi/V • Hyper-V • Baremetal • PowerVM
Cache In-Memory distribuido / DataGrid	Open: VMWare Gemfire, Oracle Coherence, Gigaspaces XAP, Hazelcast, etc.	Windows Azure Caching / Memcached	Memcached	Infinispan	WebSphere eXtreme Scale	GemFire	Ofrece IaaS, no PaaS

Fuente: (Bocchio, 2014)

2.4.8 Funcionamiento arquitectura de cloud computing

El Cloud Computing mantiene según (Pérez, 2012), una arquitectura que ofrece los servicios a los usuarios como se muestra en la Figura 20:

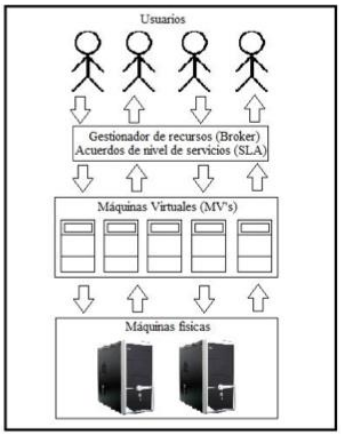


Figura 20. Arquitectura de Cloud Computing.

Fuente: (Pérez, 2012)

El usuario envía solicitudes al gestor de recursos (broker) del Data Center (Centro de Datos) del proveedor de servicios y este acuerda el nivel de servicio (SLA) que garantiza el cumplimiento de los requerimientos de usuario. El broker crea la comunicación entre

el usuario y las máquinas físicas a través de una o varias máquinas virtuales según las que requiera el usuario.

2.5 Introducción a sensor cloud.

(Niranjan Lal, 2013) define la tecnología Sensor Cloud como una infraestructura que permite la computación generalizada usando el sensor como interfaz entre el mundo físico y el virtual, el clúster de cómputo de datos como la columna vertebral cibernética y el Internet como el medio de comunicación.

De acuerdo con MicroStrain, que se encuentra entre uno de los pioneros en la invención de esta tecnología, la infraestructura de sensor cloud se define como: “Un único almacenamiento de datos de los sensores, la visualización y la plataforma de gestión remota que aprovecha las potentes tecnologías de computación en la nube para proporcionar una excelente escalabilidad de datos, visualización rápida, y el análisis programable por el usuario”, según explica (Wasai Shadab Ansari, 2012) en su investigación.

Diseñado originalmente para soportar despliegues a largo plazo de sensores inalámbricos MicroStrain, Sensor-Cloud ahora soporta cualquier dispositivo, sensor o red de sensores de terceros conectada a Internet a través de una simple API (interfaz de programación de aplicaciones) OpenData. (Wasai Shadab Ansari, 2012)

Además según (Wasai Shadab Ansari, 2012) "Una sensor cloud recoge y procesa la información de varias redes de sensores, permite compartir en gran escala la información y colaborar las aplicaciones en la nube entre los usuarios. Se integra varias redes con número de aplicaciones de detección y plataforma de cloud computing al permitir que las aplicaciones sean transversales que pueden abarcar más rangos de

organización. Sensor cloud permite a los usuarios recopilar fácilmente, el acceso, procesamiento, visualización y análisis, almacenar, compartir y búsqueda de gran cantidad de datos de los sensores de varios tipos de aplicaciones. Esta vasta cantidad de datos se almacena, procesa, analiza y luego se visualizan mediante el uso de las tecnologías de información TI computacionales y de almacenamiento recursos de la nube.

Sensor Cloud integra redes de sensores de gran escala con aplicaciones de detección e Infraestructuras de cloud computing, que recoge y procesa datos de varias redes de sensores, que permitirá el intercambio de datos a gran escala y la colaboración entre los usuarios y las aplicaciones en la nube. (Niranjan Lal, 2013)

Cada nodo sensor es programado con la aplicación requerida. Un nodo sensor también consiste de componentes de sistema operativo y componentes de administración o gestión de red. En cada nodo sensor, el programa de aplicación sensa la aplicación y luego envía hacia el gateway a través de la estación base o en multisalto a través de otros nodos. El protocolo de ruteo desempeña un rol importante en la administración de la topología de la red y para adaptar la dinámica de la red. La nube ofrece recursos de almacenamiento bajo demanda a los clientes. Esta provee acceso a los recursos a través de internet y es muy útil cuando se requiere recursos repentinamente. Combinando WSN con la nube se hace fácil el compartir y analizar datos de sensores en tiempo real. (Subasish Mohapatra, 2014)

Los sensores son utilizados por su aplicación específica para un propósito especial y esta aplicación se encarga tanto de los datos del sensor y el sensor en sí de tal manera que otras aplicaciones no pueden usar esto. Esto hace que haya desperdicio de recursos valiosos de sensores, los cuales podrían ser utilizados de manera efectiva

cuando se integra con la infraestructura de otras aplicaciones. Para llevar a cabo este escenario, se propone una infraestructura sensor cloud que puede hacer que los sensores se utilicen en una infraestructura de TI al virtualizar el sensor físico de computación en la nube. Estos sensores virtuales en una plataforma de computación en la nube son de naturaleza dinámica y, por tanto, facilitan la provisión automática de sus servicios según las necesidades de los usuarios. Además, los usuarios no tienen que preocuparse acerca de las ubicaciones físicas de múltiples sensores físicos y el espaciamiento entre los sensores físicos; en su lugar, pueden supervisar estos sensores virtuales utilizando algunas funciones estándar. (Wasai Shadab Ansari, 2012)

Para obtener QoS los sensores virtuales son supervisados regularmente para que los usuarios puedan destruir sus sensores virtuales cuando ya no se usen. Una interfaz de usuario se provee para la administración de la infraestructura sensor cloud, por ejemplo, para controlar o supervisar los sensores virtuales, provisión y eliminación de sensores virtuales, registro y borrado de sensores físicos y para la admisión de usuarios eliminadores.

(Wasai Shadab Ansari, 2012) explica que el lenguaje de modelado de sensor (SML) se puede utilizar para representar metadatos físicos de sensores como su tipo, precisión y su ubicación física, etc. También utiliza la codificación XML para los procesos de medición y descripción de los sensores físicos. Esta codificación XML para activar sensores físicos se implementan a través de varias y diferentes plataformas hardware, (OS), aplicaciones, etc., con intervención relativamente menos humana. Para transcribir las órdenes procedentes de los usuarios a los sensores virtuales y, a su vez a las órdenes de sus sensores físicos pertinentes, se realiza un mapeo entre los sensores físicos y virtuales.

La investigación reciente ha generado el concepto emergente de sensor cloud como un sustituto potencial para redes inalámbricas de sensores tradicionales (WSN). La infraestructura sensor cloud se define como una interfaz entre el mundo físico y el mundo cibernético que funciona como una plataforma para la gestión remota de datos, monitoreo y aprovisionamiento. Se trata de una nueva dimensión de la computación en la nube que se nutre de la virtualización de los nodos sensores físicos, aprovisionando de ese modo los nodos sensores físicos como un servicio bajo demanda para aplicaciones remotas. Esto permite a los usuarios finales visualizar los sensores físicos simplemente como un servicio fácil de obtener, y accesible - Sensores-as-a-Service (Se-AAS), en lugar de como un hardware típico. (Subarna Chatterjee, 2015)

En la infraestructura de sensor cloud, los nodos sensores físicos se asignan de acuerdo a la demanda de las aplicaciones en el extremo del usuario, y en consecuencia se agrupan para formar sensores virtuales (VS). Los VS además, están agrupados para formar los grupos de sensores virtuales (VSG). Se-aaS se provee a los usuarios finales a través del VS o los VSG. En el trabajo existente en sensor cloud, las aplicaciones son servidas por un procedimiento que comprende VS del conjunto máximo de los nodos sensores físicos que satisfagan los requisitos de esa aplicación. Sin embargo, teniendo en cuenta el recurso comportamiento de la red de sensores subyacente limitada, la adhesión en un VS se debe hacer de manera óptima, y de manera eficiente. Este trabajo se centra en algoritmos eficientes dinámicos, óptimos, y de recursos para la selección de los componentes de un VS, basados en la aplicación bajo demanda. (Subarna Chatterjee, 2015)

2.5.1 Características sensor cloud

En la investigación de (Beng, 2009) se describen las características de sensor cloud:

- Se integra a las redes de sensores a gran escala con aplicaciones de detección e infraestructuras de computación en la nube.
- Recoge y procesa datos de varias redes de sensores.
- Permite el intercambio de datos a gran escala y la colaboración entre los usuarios y las aplicaciones en la nube.
- Permite aplicaciones interdisciplinares que abarcan límites de la organización.
- Permite a los usuarios recoger fácilmente, acceder, procesar, visualizar, archivar, compartir y buscar grandes cantidades de datos de los sensores de diferentes aplicaciones.
- Gran cantidad de datos de los sensores puede ser procesada, analizada y almacenada utilizando recursos computacionales y de almacenamiento de la nube.
- Permite el uso compartido de los recursos del sensor por diferentes usuarios y aplicaciones en escenarios flexibles de uso.
- Habilita a los dispositivos sensores en tareas de procesamiento especializados.

2.5.2 Modelo del sistema sensor cloud

(Subasish Mohapatra, 2014) explica que una red Sensor Cloud consiste de redes de sensores inalámbricos (WSN) y recursos de la nube como computadoras, servidores, arrays de discos para procesamiento y almacenamiento de datos de sensores.

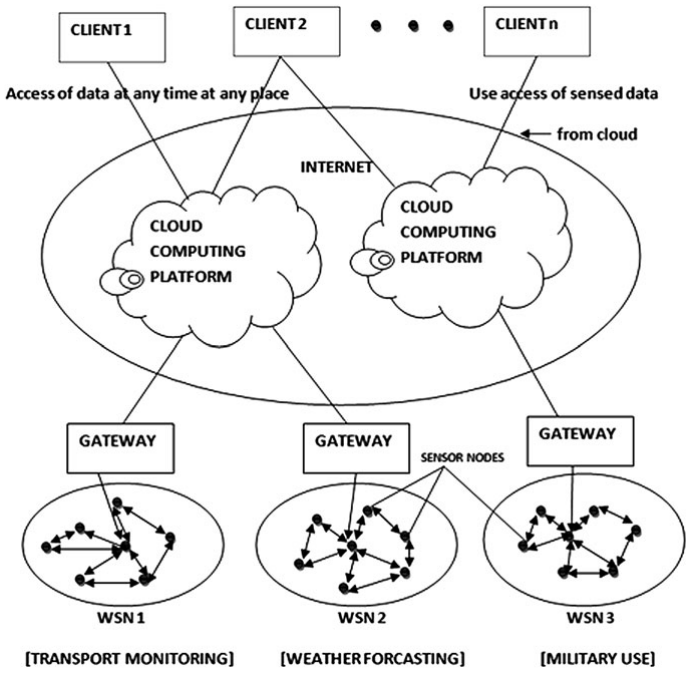


Figura 21. Modelo del sistema Sensor Cloud.

Fuente: (Subasish Mohapatra, 2014)

Los recursos en Sensor Cloud son compartidos por varias organizaciones y ciertos recursos pueden también pertenecer a más de una organización. Los usuarios de distintas organizaciones pueden acceder a los recursos Sensor Cloud, incluso si los recursos no son propiedad de su organización. La Figura 21 relacionada consta de redes inalámbricas de sensores (es decir, WSN1, WSN2, y WSN3), infraestructura de nube, y los clientes. Los clientes buscan los servicios del sistema. WSN consta de nodos de sensores inalámbricos para detectar diferentes aplicaciones fìsicas como el control del transporte, la predicción del tiempo, y las aplicaciones militares. Cada nodo sensor está programado con la aplicación requerida. El nodo sensor también se compone de los componentes del sistema operativo y los componentes de administración de red. En cada nodo sensor, el programa de aplicación detecta la solicitud y envía de vuelta al Gateway a través de la estación base o en múltiples saltos a través de otros nodos.

El protocolo de enrutamiento juega un papel vital en la gestión de la topología de red y para dar cabida a la dinámica de la red. La nube ofrece servicios y recursos de almacenamiento bajo demanda para los clientes. Proporciona acceso a estos recursos a través de Internet y es muy útil cuando hay un requisito repentino de recursos. La combinación de redes inalámbricas de sensores con la nube hace que sea fácil de compartir y analizar los datos de los sensores en tiempo real. También da una ventaja de proporcionar datos de los sensores o de eventos del sensor como un servicio en internet.

2.5.3 Arquitectura de la plataforma sensor cloud

La plataforma de sensor cloud propuesta por (Subasish Mohapatra, 2014) y (Sanjit Kumar Dash) se explica a continuación:

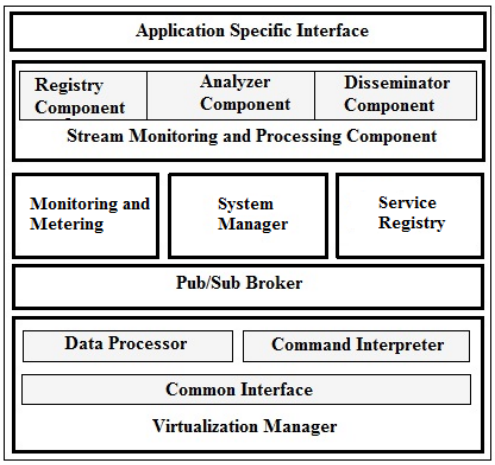


Figura 22. Arquitectura de la plataforma Sensor Cloud
Fuente: (Subasish Mohapatra, 2014) (Sanjit Kumar Dash)

A continuación se describen los componentes según se propone en (Subasish Mohapatra, 2014) y (Sanjit Kumar Dash):

2.5.3.1 Virtualization Manager - Gestor de virtualización

Este componente ayuda en la agregación de recursos autónomos y heterogéneos. Este componente se divide en 3 subcomponentes: ***Common Interface, Data processor and Command interpreter.***

1. **Common Interface (Interfaz común)**

   Las redes de sensores son conectadas por el Gateway a través de una interface común en diferentes formas (serial, usb y ethernet). El Gateway recibe los datos en bruto de los puertos de comunicación y los convierte en un paquete. El paquete es guardado en un buffer para más procesamiento.

2. **Data Processor (Procesador de datos)**

   El procesador de datos recupera los paquetes del búffer y lo procesa de acuerdo al tipo de paquete. El tipo de paquete depende de la aplicación que esté corriendo en la plataforma.

3. **Command Interpreter (Intérprete de comandos)**

   El intérprete de comandos es el responsable de proveer el canal de comunicación reversa hacia el canal del Gateway a la WSN. Este procesa e interpreta varios comandos emitidos por diferentes aplicaciones y genera el código que se entiende por los nodos sensores.

2.5.3.2 Publish/Subscriber Broker

Este módulo se encarga de la supervisión, el procesamiento y la entrega de los eventos a los usuarios registrados a través de aplicaciones de servicio (SaaS). Los componentes principales son: Stream monitoring and processing, componente de registro, componente Analizador, y componente Difusor (diseminator). (Hassan, 2009)

2.5.3.3 Monitoring and Metering - Monitoreo y Medición MaM

Este módulo rastrea el uso de los recursos de la nube. El usuario utiliza solicitudes de servicio Web autorizadas para acceder a los datos. El papel de MaM se ocupa de manejar la petición de los consumidores o usuarios, la comprobación del gestor de registro y un seguimiento de los servicios Web, etc.

2.5.3.4 System Manager- Administrador del sistema (SM)

Este módulo es responsable de procesar, archivar los datos del sensor, y la gestión de los recursos del sistema. La autenticación a la nube y control de acceso son los principales roles del gestor/administrador del sistema. Los ciclos computacionales se utilizan internamente para procesar los datos que emiten los sensores. El almacenamiento de los datos del sensor ayudará a analizar los patrones en los datos recogidos durante un período de tiempo. En general este módulo gestiona los recursos de la computadora o los servidores.

2.5.3.5 Service Registry- Registro de servicio

Mantiene las credenciales de diferentes aplicaciones del usuario en el sistema de editor/ suscriptor.

2.5.3.6 Monitoreo y procesamiento de Streams (SMP)-Stream Monitoring and Processing.

SMP supervisa las tramas o streams de sensores que viene en muchas formas, desde diferentes fuentes e invoca el método correcto de análisis. Este módulo se divide en tres subcomponentes, es decir, el componente del registro, componente analizador, y el componente diseminador o difusor.

Dependiendo de las velocidades de datos y la cantidad de procesamiento que se requiere, SMP gestiona el modelo de ejecución paralelo en Cloud. (Hassan, 2009)

1. *Registry Component (RC)*- **Componente del Registro (RC)**

Registros de suscripciones de usuarios de diferentes aplicaciones y datos de sensores específicos del usuario. También envía todas las suscripciones de los usuarios, junto con ID de aplicación al componente **difusor** para la entrega del evento. (Hassan, 2009)

Para cada aplicación, el componente de registro almacena las suscripciones de usuarios, datos de los sensores, y el tipo de evento del sensor. Cada aplicación está asociada con un ID de aplicación único, junto con el acuerdo de nivel de servicio service level agreemment (SLA). SLA proporciona la base para la medición y contabilidad de los servicios que se utilizará cubriendo todos los atributos de los clientes.

2. *Analyzer Component (AC)* **Componente Analizador**

Este analiza los datos de los sensores de entrada o evento para que coincida con las suscripciones de usuario en el registro de servicios. Si los datos del sensor coinciden con el interés del abonado, el mismo es entregado al componente difusor para entregar a los usuarios adecuados.

3. *Disseminator Component (DC)* **Componente diseminador o difusor (DC)**

Recibe los datos o evento de interés a partir del componente analizador y entrega los datos a través de interfaz de la aplicación al suscriptor o abonado.

2.5.3.7 Virtual machine manager (VMM)

El objetivo de este componente es mejorar la utilización de los recursos, proporcionando una plataforma integrada unificada para la aplicación por usuario basada en la agregación de recursos heterogéneos y autónomos. También es importante como una forma de mejorar la seguridad del sistema, fiabilidad, disponibilidad, y una mayor flexibilidad con menor coste. El monitor de máquina virtual (VMM) permite a la máquina física ser virtualizado en diferentes máquinas virtuales (VM). VMM divide los recursos físicos y brinda un entorno multi-servidor escalable que está completamente virtualizado

con todos los recursos. Las instancias de máquinas virtuales comparten hardware común como almacenamiento, memoria, E/S, el software de información, y los servidores.

Estas técnicas proporcionan aislamiento completo entre las máquinas virtuales y permiten la instalación de igual o diferente sistema operativo en diferentes máquinas virtuales. Diferentes aspectos de la virtualización son tales como la virtualización completa, la virtualización del sistema operativo, la para-virtualización, y la virtualización H/W. La virtualización completa utiliza un tipo especial de software llamada hipervisor. El Hypervisor directamente interactúa con el servidor físico y mantiene cada servidor virtual totalmente independiente y consciente de los otros servidores virtuales que se ejecutan en la máquina física. Cada servidor invitado se ejecuta en su propio sistema operativo. Pero en el sistema de para-virtualización, el servidor de invitados tiene conocimiento de otro servidor. Es un subconjunto de la virtualización de servidores. Los dispositivos que interactúan en entorno de para-virtualización es muy similar a los dispositivos de interacción en entorno virtualizado completo. En otra parte, la virtualización del sistema operativo también se conoce como virtualización basada en contenedores. Implementa la virtualización mediante la ejecución de más instancias del mismo sistema operativo en paralelo. La virtualización H/W se utiliza comúnmente en el servidor debido al alto aislamiento de la máquina virtual y el rendimiento.

2.5.3.8 Application Specific Interface - Interface de aplicación específica

Esta interfaz brinda flexibilidad a los vendedores (proveedores) para acceder a servicios alojados en la nube de sensores de forma remota a través de Internet. Este modelo tiene como objetivo llevar los datos del sensor a un agente de publicación/subscripción a través de gateways. El agente de publicación/ subscripción proporciona información

a los consumidores de las interfaces de aplicaciones. Los servicios Web de la plataforma sensor cloud tienen acceso a través de las interfaces integradas con las tecnologías Web 2.0. Las diversas aplicaciones SaaS transfieren la información y las suscripciones de los usuarios registrados al registro del agente de publicación/ subscripión.

Las interfaces permiten el acceso a los servicios web de la plataforma WSN cloud. Los consumidores pueden consumir los servicios a través de servicios web que a menudo se hace referencia como interfaz de programación de aplicaciones de Internet (IAPI). Esto permite a los usuarios acceder a los servicios alojados de forma remota a través de la red, como Internet.

Los procesos de registro y suscripción según (Subasish Mohapatra, 2014) se explican a continuación:

2.5.4 Registro del proveedor:

Cuando el usuario quiere suscribir los eventos de interés a través de un agente, debe registrarse al agente con la identificación del cliente, la dirección IP y el puerto. Los vendedores envían mensajes asociados **[ID de cliente, IP y puerto]** al agente para nuevas conexiones. Los clientes pueden cambiar su agente a uno con mejores facilidades como conexión de radio y reconexión automática. Si son mayores, entonces se asocian con el mensaje **[ID de cliente, IP, puerto, último ID agente].** Cuando el agente recibe la solicitud, se asigna un bloque de memoria en su almacenamiento local para almacenar los detalles del cliente. El componente de registro almacena suscripciones de usuarios de diferentes aplicaciones y datos específicos del usuario y los tipos de los vendedores que se registren a un agente de publicación/ subscripción.

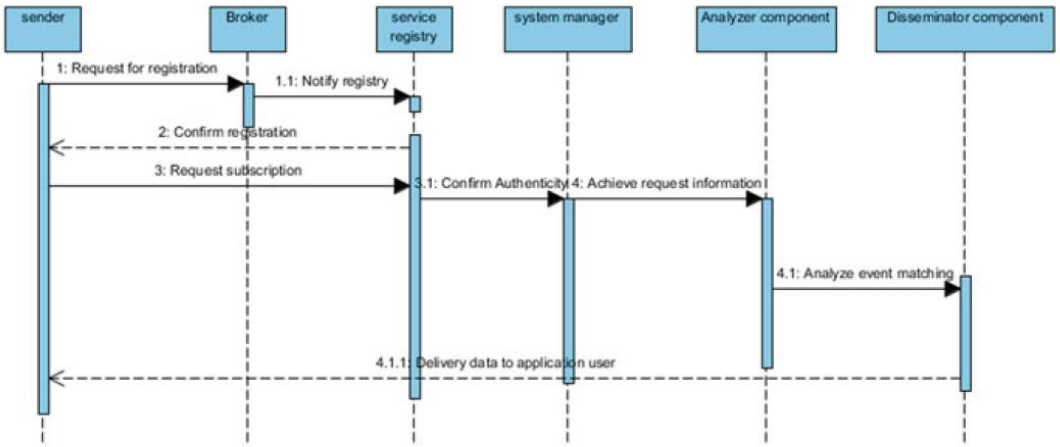


Figura 23. Diagrama de secuencia para el modelo de entrega de datos de sensor cloud.
Fuente: (Subasish Mohapatra, 2014)

2.5.5 Suscripción del Proveedor

Después del registro de los proveedores, que solicitan para la suscripción como **[sub ID, ID de evento, área, filtros]** donde sub ID es el único ID de suscripción para los proveedores. El identificador de evento es la respuesta a un evento correspondiente a una solicitud que ha sido publicada en el sistema. El **Área** describe la ubicación de destino en el que el abonado tiene interés. Los filtros se utilizan para extraer la información relevante que se envía al suscriptor. Los vendedores después de su inscripción envían su mensaje de suscripción al **broker**. El **broker** agrega este ID con el mensaje del suscriptor y envía al almacenamiento de la nube, de lo contrario el agente que se encuentra en la ubicación de destino especificada en el mensaje. Con la ayuda de un algoritmo de enrutamiento, el agente accede a los datos de manera eficiente. El diagrama de secuencia (Figura 23) explica el registro de proveedores y suscripción en detalle.

2.5.6 Modelo del sistema sensor cloud

En (Sanjit Kumar Dash) se explica el modelo sensor cloud, que tiene como objetivo llevar los datos del sensor a un agente de publicación/subscripción a través de gateways. El agente de publicación/ subscripción proporciona información a los consumidores de las interfaces de aplicaciones. A los servicios web de la plataforma WSN cloud se les concede acceso (tienen acceso garantizado) a través de las interfaces integradas con las tecnologías Web 2.0. El enmascaramiento de los datos de nivel inferior de cada nube WSN en términos de diferentes plataformas, sensores utilizados, y los datos que se generan se realiza mediante el administrador de virtualización (Virtualization Manager). Las diversas aplicaciones SaaS transfieren la información y las suscripciones de los usuarios registrados al componente de Registro del agente de publicación/ suscripción**.** Los datos de sensores, al llegar al sistema desde los gateways, se determinan a continuación, a través del componente stream monitoring and processing (SMPC) en el agente de publicación/ suscripción en cuanto a si necesitan procesamiento o simplemente tienen que ser almacenados para entrega periódica o para entrega inmediata. Si en caso los datos de los sensores necesitan la entrega periódica, el analizador determina qué aplicaciones SaaS insertan los eventos y pasan luego a los sucesos al difusor (disseminator).

El difusor (disseminator) luego entrega los eventos para su uso mediante la búsqueda de los suscriptores adecuados para cada aplicación con la ayuda del algoritmo de coincidencia de eventos. Los ciclos de cómputo se proporcionan internamente por **SM** (System Manager) según sea necesario para procesar los datos emanados de los sensores. **SRM** gestiona suscripciones y credenciales de los usuarios. **MaM** (Monitoring and Metering) calcula el precio de los servicios ofrecidos**.**

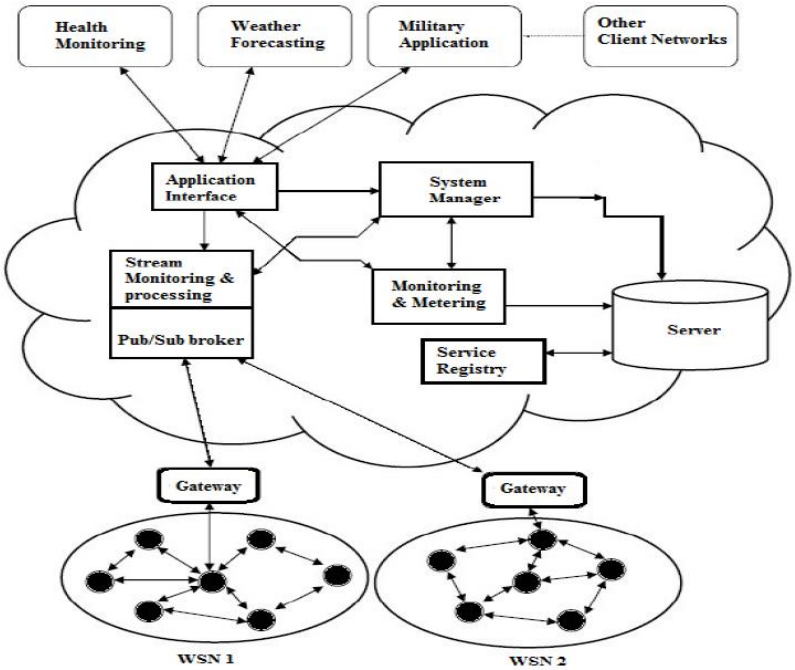


Figura 24. Modelo Sensor Cloud

Fuente: (Sanjit Kumar Dash)

2.5.7 Consideraciones de diseño

Hay diversos sensores físicos pertenecientes a diferentes propietarios. Cuando una aplicación o middleware tiene que utilizar algunos sensores, los sensores necesarios deben organizarse de forma dinámica. A continuación se explican algunas consideraciones de diseño propuestas por (Madoka Yuriyama, 2010) y que deben ser tomadas en cuenta:

1. **Virtualización**

Hay varios tipos de sensores físicos dispersos. Proponemos un sensor virtual y un grupo de sensores virtuales para que los usuarios puedan utilizar sensores sin tener que preocuparse acerca de los lugares y las especificaciones de sensores físicos.

Cada sensor virtual se crea a partir de uno o más sensores físicos. Un grupo sensor virtual se crea a partir de uno o más sensores virtuales. Los usuarios pueden crear grupos de sensores virtuales y utilizar libremente los sensores virtuales incluidos los grupos como si fueran propiedad de sensores. Por ejemplo, se pueden activar o desactivar los sensores virtuales, comprobar su estado, y establecer la frecuencia de recolección de datos de ellos. Si varios usuarios controlan libremente los sensores físicos, algunos comandos inconsistentes pueden ser emitidos. Los usuarios pueden controlar libremente sus propios sensores virtuales mediante la virtualización de los sensores físicos como sensores virtuales.

2. Estandarización

Diferentes tipos de sensores físicos tienen diferentes especificaciones. Cada sensor físico ofrece sus propias funciones de control y recogida de datos. Un mecanismo estándar permite a los usuarios acceder a los sensores sin la preocupación por las diferencias entre los sensores físicos. Definimos las funciones estándar de sensores virtuales, por lo que los usuarios pueden acceder a los sensores virtuales con las funciones estandarizadas. La infraestructura Sensor-Cloud traduce las funciones estándar para los sensores virtuales en funciones específicas para los diferentes tipos de sensores físicos.

3. Automatización

La automatización mejora el tiempo de prestación de servicios y reduce el coste. Si hay operaciones que involucran seres humanos, esos servicios serán lentos y costosos. La Infraestructura Sensor-Cloud prepara el modelo para las especificaciones de varios sensores físicos. Cuando los usuarios seleccionan el modelo de un sensor virtual o grupo de sensores virtuales, la infraestructura Sensor-Cloud dinámica y

automáticamente provee los sensores virtuales en ese grupo de sensor virtual a partir del modelo especificado. La infraestructura Sensor-Cloud es una prestación de servicios bajo demanda y apoya el ciclo de vida completo de la prestación de servicios a partir del registro de sensores físicos a través de la creación de modelos o plantillas, solicitando de sensores virtuales, aprovisionamiento, inicialización, finalización de uso de sensores virtuales y eliminación de sensores físicos. Estas formas de apoyo son automáticas y se entregan sin operaciones humanas.

4. Monitoreo

Debido a que la aplicación tiene problemas si no puede utilizar los datos de los sensores virtuales, el propietario de la aplicación debe comprobar si los sensores virtuales están disponibles y controlar su estado para mantenimiento de la calidad del servicio. Los usuarios pueden comprobar el estado y la disponibilidad de los sensores virtuales por el mecanismo de monitoreo de la infraestructura Sensor-Cloud.

5. Agrupación

Aunque hay muchos tipos de sensores físicos, cada aplicación no tiene que utilizar todos ellos. Cada aplicación utiliza algunos tipos de sensores o cuando los sensores que responden a ciertas restricciones (tales como una ubicación). La infraestructura Sensor-Cloud puede proporcionar sensores virtuales como grupos de sensores virtuales. Los usuarios pueden controlar cada sensor virtual y grupos de sensores virtuales. Por ejemplo, un usuario puede establecer el control de acceso y la frecuencia de recolección de datos para grupos de sensores virtuales. La infraestructura Sensor-Cloud prepara grupos típicos de sensores virtuales y los usuarios pueden crear nuevos grupos de sensores virtuales mediante la selección de sensores virtuales.

6. **Modelo de servicio:**

Cuando los sensores físicos son sólo para una aplicación especializada, cada aplicación puede utilizar y gestionar libremente sus propios sensores físicos. La infraestructura Sensor-Cloud proporciona la infraestructura para compartir diversos sensores como un servicio. La infraestructura Sensor-Cloud es responsable de mantener la calidad del servicio. Nos define los roles asignados a los participantes al unirse al servicio, teniendo en cuenta sus méritos y la creación de un modelo de costos adecuada para soportar el servicio.

2.5.8 Actores en la infraestructura sensor cloud

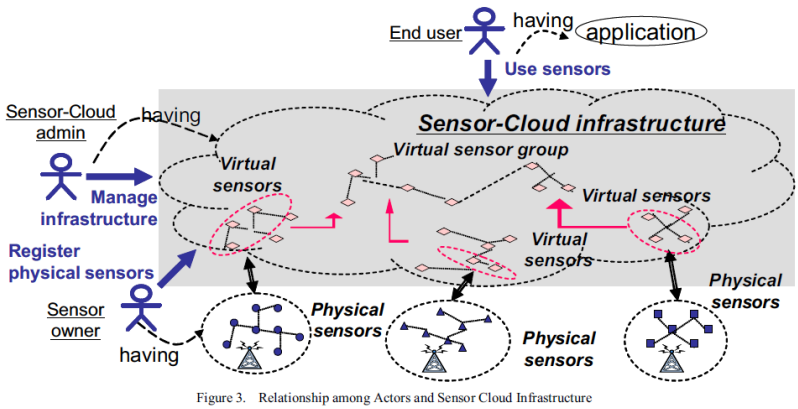


Figura 25. Relación entre los actores y la infraestructura Sensor Cloud.

Fuente: (Madoka Yuriyama, 2010)

A continuación se muestra las relaciones entre los actores y la infraestructura según (Madoka Yuriyama, 2010):

1. **Sensor Propietario:** Es un actor que posee sensores físicos. El sensor propietario permite que otros utilicen esos sensores físicos a través de la infraestructura de Sensor Cloud. Una de las posibles ventajas para el sensor propietario podrían ser las tasas de alquiler para el uso de los sensores físicos.

Los honorarios refleja el uso real de los sensores físicos. El sensor propietario registra los sensores físicos con sus propiedades en la infraestructura Sensor-Cloud. El propietario borra el registro de ellos cuando él les deja de compartir.

2. **Administrador Sensor-Cloud:** El Administrador Sensor-Cloud es el actor que gestiona el servicio de Infraestructura Sensor-Cloud. El administrador gestiona los recursos de TI para los sensores virtuales, monitoreo y las interfaces de usuario. El administrador también prepara los modelos para los sensores virtuales y para algunos grupos de sensores virtuales típicos. El administrador puede cobrar por la prestación del servicio de infraestructura Sensor-Cloud.

3. **Usuario final:** Un usuario final es un actor con una o más aplicaciones o servicios que utilizan los datos del sensor. Un usuario final solicita el uso de sensores virtuales o grupos de sensores virtuales que cumplan los requisitos de los modelos. Los modelos o plantillas son preparados por administradores Sensor-Cloud. El usuario también puede crear una nueva plantilla o modelo del grupo de sensores virtuales o mediante la modificación de la plantilla existente del grupo sensor virtual o por sus propios sensores virtuales activos. Los usuarios pueden compartir sus propias plantillas entre otros usuarios finales. El usuario puede controlar sus sensores virtuales directamente o a través de un navegador Web. El usuario puede monitorizar el estado de los sensores virtuales. Cuando se convierten en no necesarias, el usuario puede liberarse de ellos. Los usuarios finales pueden utilizar los sensores virtuales mediante el pago para el uso y sin un conocimiento detallado de los sensores físicos.

(Madoka Yuriyama, 2010) define los tres tipos de actores de acuerdo a los roles en la infraestructura Sensor-Cloud. Cuando se entregan los servicios de infraestructura Sensor-Cloud, la misma persona u organización pueden tener al mismo tiempo los papeles de propietario y administrador Sensor-Cloud, en especial cuando hay sólo unos pocos tipos de sensores físicos que son propiedad de una organización. El sistema es más escalable si el administrador de sensor Cloud es diferente de los propietarios de los sensores. El administrador de Sensor-Cloud se centra en la fiabilidad y la calidad del servicio.

2.5.9 Ventajas de sensor cloud

A continuación según (Wasai Shadab Ansari, 2012) se describen las diversas ventajas y beneficios de la infraestructura sensor cloud:

2.5.9.1 Análisis:

La integración de datos de sensores enormemente acumulados de varias redes de sensores y el modelo cloud computing hace que sea atractivo para los diversos tipos de análisis requeridos a los usuarios mediante el aprovisionamiento de la escalabilidad de potencia de procesamiento.

2.5.9.2 Escalabilidad:

Sensor-Cloud permite a las redes de sensores anteriores escalar en tamaño muy grande debido a la gran arquitectura de enrutamiento de la nube. Esto significa que a medida que aumenta la necesidad de recursos, las organizaciones pueden ampliarse o añadir los servicios adicionales de proveedores de computación en la nube sin tener dinero extra para estos recursos de hardware adicionales.

2.5.9.3 Colaboración

Sensor-cloud permite a los datos de los sensores grandes ser compartidos por diferentes grupos de consumidores a través de la colaboración de varias redes de sensores físicos. Se facilita la colaboración entre los distintos usuarios y aplicaciones para el intercambio de datos enormes en la nube.

2.5.9.4 Visualización

Plataforma sensor-cloud proporciona una API de visualización para ser utilizado para la representación de los diagramas con los datos de sensor almacenados y recuperados de varios activos de dispositivos. A través de las herramientas de visualización, los usuarios pueden predecir las posibles tendencias futuras que tienen que ser incurridos.

2.5.9.5 Aprovisionamiento gratuito de mayor capacidad de almacenamiento de datos y capacidad de procesamiento

Proporciona almacenamiento de datos disponible y las organizaciones pueden poner sus datos en lugar de poner en sistemas informáticos privados sin ser molestado. Se ofrece enormes recursos de las instalaciones de almacenamiento y procesamiento para manejar los datos de aplicaciones a gran escala.

2.5.9.6 Aprovisionamiento dinámico de los servicios

Los usuarios de sensor-cloud pueden acceder a su información relevante desde cualquier lugar que desee y cada vez que necesite.

2.5.9.7 Multi-arrendamiento

Número de servicios de varios proveedores de servicios pueden ser integrados fácilmente a través de la nube e Internet para numerosos servicios de innovación para satisfacer la demanda de los usuarios. Sensor-Cloud permite el acceso a varios números de centro de datos ubicado en cualquier parte de la red global.

2.5.9.8 Reducción de costos y mayores ganancias

La integración de sensores con la nube permite reducir el costo de los recursos de forma incremental y lograr mayores ganancias de los servicios. Con sensor-cloud tanto de la pequeña y mediana empresa pueden obtener todos los beneficios de una enorme infraestructura de recursos sin tener que involucrar y administrarlo directamente.

2.5.9.9 Automatización

La automatización juega un papel vital en la provisión de servicios de computación sensor-cloud. La automatización de servicios mejora el tiempo de entrega, en gran medida.

2.5.9.10Flexibilidad

Sensor-Cloud ofrece más flexibilidad a sus usuarios que los métodos de computación pasados. Proporciona flexibilidad para utilizar las aplicaciones al azar cualquier número de veces y permite compartir los recursos de sensores en un entorno de uso flexible.

2.5.9.11Agilidad de los servicios

Sensor-Cloud proporciona servicios ágiles y los usuarios son capaces de ser aprovisionados con los costosos recursos de infraestructura tecnológica con menos gasto. La integración de las redes de sensores inalámbricos con la nube permite alta velocidad de procesamiento de datos utilizando inmensa capacidad de procesamiento de la nube.

2.5.9.12Optimización de recursos

La infraestructura del sensor en la nube permite la optimización de recursos al permitir la puesta en común de recursos para varios números de las aplicaciones.

2.5.9.13Tiempo de reacción rápida

La integración de WSN con la nube proporciona una respuesta muy rápida para el usuario, es decir, en tiempo real debido a la gran arquitectura de enrutamiento de la nube. El tiempo de respuesta rápida de los datos se alimenta de varias redes de sensores o dispositivos permiten tomar decisiones críticas en tiempo real.

2.5.10 Desventajas de sensor cloud

Según (Wasai Shadab Ansari, 2012) las desventajas de la infraestructura sensor cloud son las siguientes:

- Sensor cloud requiere un sistema de gestión muy amplio con el fin de realizar un seguimiento de los usuarios finales, los recursos de TI, Sensores virtuales, sensores físicos, etc.
- La infraestructura de Sensor cloud es vulnerable y más propensa a sofisticados ataques distribuidos de intrusión como DDoS (Denegación de Servicio Distribuir) y XSS (Cross Site Scripting).
- Es necesario buscar una conectividad continua de datos entre los usuarios finales y el servidor de sensor-cloud.

2.5.11 Problemas y retos durante el diseño de la infraestructura sensor-cloud

Según la investigación de (Wasai Shadab Ansari, 2012) existen varios problemas como problemas de diseño, de ingeniería, conexión fiable, el flujo continuo de datos, alimentación, etc., que se deben considerar para el diseño de una infraestructura sensor cloud:

1. **Algunas cuestiones de ingeniería**, como el almacenamiento de los datos del lado del servidor, la transferencia de datos desde el teléfono al servidor debe

tener para ser considerado. Para hacer frente a esta de las marcas de tiempo se envían con cada paquete de datos para ayudar en la reconstrucción de los datos en el lado del servidor. La mayor parte del procesamiento de datos se realiza en el extremo del servidor por lo que el sistema debe estar diseñado para evitar el procesamiento de ráfagas debido a múltiples usuarios conectados simultáneamente al sistema. El sistema debe estar diseñado para dar cabida a múltiples usuarios se conecten al mismo tiempo.

2. **Una interfaz de usuario basada en web se utiliza** por lo que el sistema debe tener para ofrecer diferentes funciones de autorización para diferentes tipos de usuarios y autenticado a través de esta interfaz web. Esto permitirá privacidad en cierta medida, al permitir que los cuidadores limitarlos a un solo paciente que él / ella va a cuidar.
3. **El procesamiento de eventos y administración**: Sensor-Cloud tiene que hacer frente a medios de tratamiento y gestión de eventos muy complejos.

   Cómo deben sincronizarse los sucesos que pueden provenir de fuentes diferentes en tiempo diferente debido a retrasos en la red

   -¿Cómo las reglas de procesamiento de eventos tienen que cambiar sin afectar el sistema?

   -¿Cómo se soportan los mensajes y eventos de diferentes tipos?

   ¿Cómo apoyar de manera óptima el enorme número de eventos y sus condiciones?

   ¿Cómo podemos reconocer el contexto (es decir, espacial, temporal, semántico) a su detección de la situación relevante?
4. **Violación del acuerdo de Nivel de Servicio (SLA):** La dependencia de los consumidores en los proveedores de la nube para sus aplicaciones en necesidades de computación (como su procesamiento, almacenamiento,

análisis de los enormes datos del sensor y datos generados por los usuarios) en demanda, puede requerir una determinada calidad de servicio a mantenerse para las solicitudes sostenibilidad del usuario y para cumplir con sus objetivos. Pero, si los proveedores cloud que no pueden proporcionar estos servicios de calidad en la demanda del usuario pueden estar en caso de procesamiento de datos de los sensores enormes en situaciones ambientales críticas, debería resultar en violación de SLA y el proveedor debe ser responsable. Por lo tanto, necesitamos una colaboración dinámica fiable entre los proveedores cloud. Pero optar por la mejor combinación de los proveedores cloud en colaboración dinámica es gran desafío en términos de costo, tiempo, discrepancia entre los proveedores y calidad de servicio.

5. **Necesidad de difusión de información eficiente:** En sensor cloud necesitamos un mecanismo de difusión de información eficiente que puede coincidir con los eventos publicados o datos de los sensores a las aplicaciones de usuario apropiadas. Sin embargo, puede haber algunas cuestiones como el mantenimiento de la flexibilidad en la prestación de un poderoso esquema de suscripción que puede capturar información acerca de eventos, lo que garantiza la escalabilidad con respecto al número de abonados y eventos publicados o datos de los sensores, etc. Dado que los conjuntos de datos y sus servicios de acceso pertinentes se distribuyen geográficamente, la asignación de almacenamiento y difusión de datos se convierte en desafíos críticos.
6. **Las cuestiones de soporte de seguridad y privacidad:** Hay menos estándares disponibles para garantizar la integridad de los datos en respuesta a cambios debido a las transacciones autorizadas. Los consumidores necesitan saber si su / sus datos en el centro de la nube es así cifrada o que supervisan las claves de cifrado / descifrado (es decir, la nube del proveedor / cliente en sí).

Los datos privados de salud pública pueden llegar a ser causa de error o inexactitud es decir, la privacidad del consumidor puede perderse en la nube y los sensores de datos o información cargada en nube no pueden ser supervisados correctamente por el usuario.

7. **Procesamiento de contenido multimedia en tiempo real y la escala masiva:** El uso de gran cantidad de información en tiempo real y su minería es un gran desafío en la integración de fuentes de datos heterogéneas y masivas con la nube. Para clasificar esta información en tiempo real los contenidos multimedia y de modo que puede desencadenar a los servicios pertinentes y ayudar al usuario a su ubicación actual es también un gran reto para ser manipulados.
8. **Recolección de Inteligencia Colectiva:** La alimentación de los datos del sensor en tiempo real heterogénea mejora la capacidad de toma de decisiones mediante el uso de los datos adecuados y mecanismos de fusión a nivel de decisión. Sin embargo, la maximización de la inteligencia desarrollada a partir de la información de forma masiva con ubicación en la nube sigue siendo un reto muy grande.
9. **Los problemas de eficiencia energética:** Con el fin de extender la independencia del sistema, la eficiencia de energía de tales sistemas (sensores textiles y microcontrolador basado) es principal problema que tiene que ser manejado.
    a. El mecanismo de almacenamiento en caché de datos [49] también se puede utilizar para volver a utilizar los datos pasados del sensor para aplicaciones que son tolerantes a tiempo, es decir constante, por ejemplo, una aplicación relacionada con la temperatura ambiente variante etc. Si usamos estos datos pasados del sensor para satisfacer

las diversas solicitudes de datos de los sensores comunes, el consumo de energía se reducirá.

10. **Limitación de ancho de banda:** la limitación de ancho de banda es uno de los grandes desafíos actuales que tiene que manejar en el sistema de infraestructura sensor cloud debido a que el número de dispositivos sensores y sus usuarios de la nube se incrementan dramáticamente alta. Sin embargo hay un número de métodos óptimos y eficientes de asignación de ancho de banda propuesto, pero para gestionar la asignación de ancho de banda con una infraestructura tan gigantesca que consiste en enormes activos de dispositivos y usuarios de la nube, la tarea de asignación de ancho de banda para cada dispositivo y usuarios se vuelve casi difícil.
11. **Red de gestión de acceso:** Tenemos varios y múltiple número de redes de tratar en aplicaciones de arquitectura de sensor-cloud. Así que necesitamos un esquema de administración de acceso adecuado y eficiente para estos varios números de las redes, ya que esto optimiza el uso del ancho de banda y rendimiento mejorando enlaces.
12. **Temas de precios:** Para acceder a los servicios de sensor cloud implica tanto el proveedor de servicios Sensor (SSP) y el proveedor de servicios cloud (CSP). Sin embargo, ambos SSP y CSP tienen diferente administración de clientes, gestión de servicios, modo y métodos de pagos y precios. Por lo tanto, todo esto conducirá serie de cuestiones como: ¿Cómo fijar el precio?, ¿Cómo fue hecho el pago a los clientes?, ¿Cómo se distribuirá el precio entre las diferentes entidades?, etc.
13. **Problemas de estandarización de interfaz:** las interfaces Web actualmente proporcionan la interfaz entre los usuarios de sensor cloud y en la nube. Pero la interfaz web puede causar sobrecarga porque las interfaces Web no están

diseñadas específicamente para teléfonos inteligentes o dispositivos móviles. Además, no habría problemas de compatibilidad de la interfaz web de los dispositivos y en este caso la señalización, el protocolo estándar, y la interfaz para interactuar entre los usuarios de sensor cloud y la nube requeriría servicios integrados para la implementación. Por lo tanto, la interoperabilidad sería un gran problema cuando los usuarios de sensor-cloud necesiten acceder a los servicios con la nube.

2.5.12 Modelo de la arquitectura sensor cloud

En la Figura 26 a continuación se muestra el modelo propuesto por (Shah, 2013), en el que se integran WSN y Cloud Computing. Los componentes del modelo incluyen: Unidad de Procesamiento de Datos (PDU), Pub /sub broker, Solicitud de Abonado (RS), Identidad y Unidad de Gestión de Acceso (IAMU), y el Repositorio de datos (DR). Los datos recogidos de la WSN se mueven a través de un gateway a la PDU. La PDU (Unidad de procesamiento de datos) procesará los datos en un formato de almacenamiento y luego enviará los datos al DR (Data Repository).

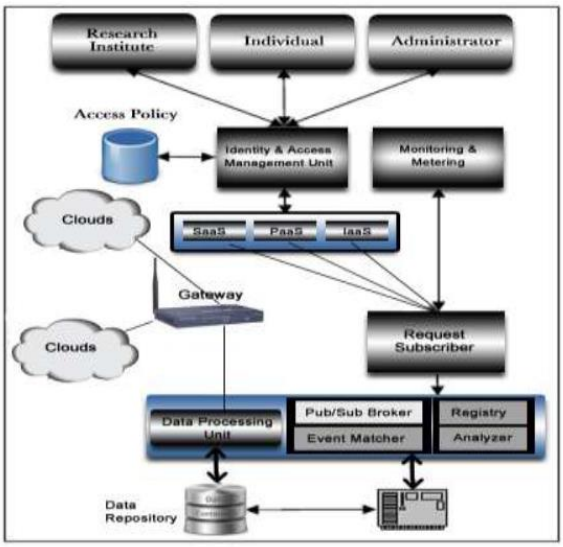


Figura 26. Modelo de integración Sensor Cloud

Fuente: (Shah, 2013)

En referencia al funcionamiento (Khandakar Entenam Unayes Ahmed, 2014) explica que los usuarios se conectan a la nube a través de la **IAMU (Identity and Acces Management Unit)** segura y se le concede acceso en base a la política almacenada en su cuenta de usuario. Una vez que se ha concedido el acceso, los usuarios pueden presentar solicitudes de acceso a datos. Las solicitudes serán enviadas a la **RS (Request Subscriber)** y **RS** creará una suscripción sobre la base de esta solicitud y remitirá esta suscripción al **pub/ sub Broker**. Los datos recibidos en la nube serán identificados por la **PDU (Data Processing Unit - unidad de procesamiento de datos)** que creará un evento de datos publicado y enviará el evento a una cola de eventos en el **Pub/ Sub Broker**. Cuando se publica un nuevo evento, cada suscripción se evalúa por el componente de **coincidencia de eventos (Event matcher/ Disseminator)** una vez que el proceso de coincidencia de eventos encuentra una coincidencia.

A. Identity and Access Management Unit:

Según (Khandakar Entenam Unayes Ahmed, 2014) cuando el usuario requiere información de la Plataforma Sensor Cloud, se conecta a la aplicación específica SaaS a través del IAMU, la cual se encarga de proporcionar autenticación fuerte entre el cliente y el proveedor, además de proporcionar a los recursos de la nube un control de acceso basado en políticas, como mecanismos de seguridad.

El sistema **IAMU** incluye dos componentes principales: Unidad de Control de Acceso (**ACEU**); y Unidad de Decisión de Control de Acceso (**ACDU**). Se implementa la autenticación Kerberos introduciendo una nueva unidad llamada Edge Node (EN) que también implementa el algoritmo de clave pública Diffie-Hellman.

El prototipo de Identity and Access Management Unit (**IAMU**) incluye **Diffie Hellman, Kerberos**, Control de Acceso Basado en Función (Role Based Access Control) (**RBAC**) y Extensible Markup Language (**XML**).

A continuación se ilustra un diagrama esquemático de IAMU.

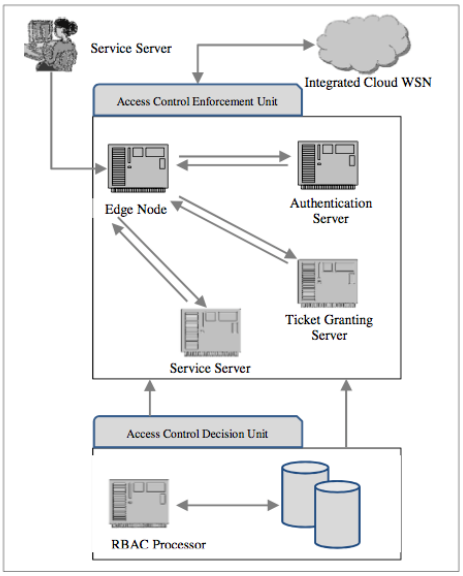


Figura 27. Diagrama esquemático del Sistema General IAMU

Fuente: (Khandakar Entenam Unayes Ahmed, 2014)

1) Access Control Enforcement Unit / Unidad de Control de Acceso de Aplicación

ACEU se utiliza para autenticar al usuario. El ACEU consta del Nodo Edge (EN) y tres servidores: Authentication Server (AS), Ticket Granting Server (TGS) y Service Server (SS). Una solicitud llega a la EN y luego va al AS. La petición recibida por EN se envía al AS. EN implementa Kerberos para autenticar el cliente con el AS. (Shah, 2013)

2) Access Control Decision Unit/ Unidad de Decisión de Control de Acceso

ACDU se utiliza para hacer cumplir las reglas de política. Consta de procesador de RBAC y almacenamiento de políticas. Se comunica con ACEU través SS. Después de

la autenticación exitosa; usuario se le da el acceso a los recursos como restringido por las políticas de acceso. (Shah, 2013)

La ACDU consiste en el procesador RBAC y el almacenamiento de políticas de usuario. La ACDU se comunicará con el ACEU a través del SS.

El proceso de autenticación asocia a los usuarios con directivas de acceso y, una vez completado este proceso, el usuario obtiene acceso a los recursos de datos dentro de las limitaciones impuestas por las políticas de acceso. El modelo propuesto incluye control, gestión de grupos y usuarios y otra información que se almacena utilizando XML. (Khandakar Entenam Unayes Ahmed, 2014)

3) Flujo de Interacción entre el usuario y IAMU

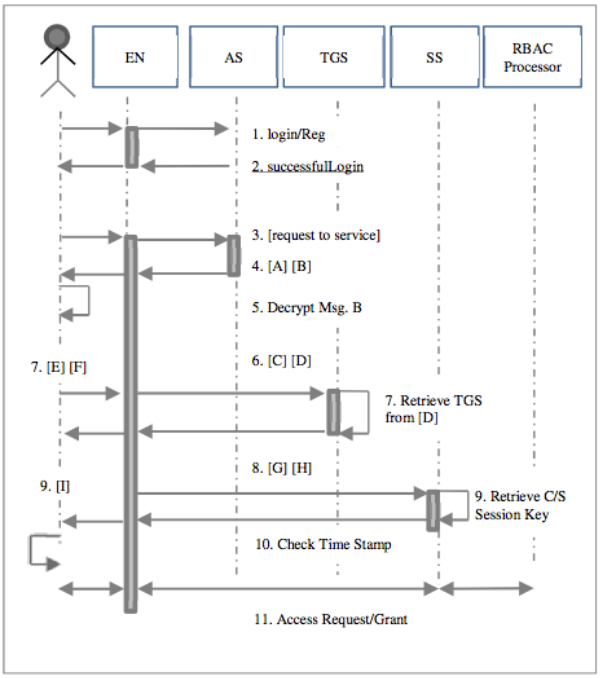


Figura 28. Diagrama de Secuencia IAMU

Fuente: (Khandakar Entenam Unayes Ahmed, 2014)

A continuación según (Khandakar Entenam Unayes Ahmed, 2014) se muestra los

pasos involucrados en el IAMU:

1. Login de un usuario anterior o registro de un usuario nuevo. Este inicio de sesión / registro ocurre de forma segura cifrado por la clave o algoritmo de Diffie-Hellman.

2. Recibe el reconocimiento (ACK) de la conexión correcta. (Pasos o proceso de autenticación)

3. El nodo Edge (EN) envía un mensaje [request to service] al **AS** solicitando servicios en nombre del usuario.

4. Después de recibir la solicitud de servicio de un cliente **AS** generará dos mensajes siguientes y los enviará al cliente vía **EN**.

a. Mensaje A: Client / TGS Session Key que se cifra usando la clave pública del cliente / usuario.
b. Mensaje B: Ticket TGT que incluye ID de cliente, dirección de red de cliente, período de validez de ticket y Clave de Sesión de Cliente / TGS, cifrado usando la clave secreta del TGS.

5. Después de recibir los mensajes A y B de AS, el Cliente descifrará el mensaje A para obtener la clave de sesión Client / TGS. Esta clave de sesión se utiliza para comunicaciones adicionales con TGS.

Pasos para la autorización del servicio al cliente

6. Ahora, el cliente enviará los siguientes dos mensajes a TGS:

A. Mensaje C: Compuesto por el TGT del mensaje B y el ID del servicio solicitado.

B. Mensaje D: Id. De cliente y la marca de tiempo cifrada utilizando la clave de sesión de cliente / TGS (autenticador).

7. Al recibir los mensajes C y D, el TGS recupera TGT del mensaje C. Descifra TGT usando la clave secreta TGS. Esto le da la Clave de Sesión de Cliente / TGS. Utilizando esta clave, el TGS descifra el mensaje D (Authenticator) y envía los dos mensajes

siguientes al cliente:

A. Mensaje E: ticket cliente a servidor (que incluye el ID del cliente, la dirección de red del cliente, el período de validez y la clave de sesión cliente / servidor) cifrados mediante la clave secreta SS.

B. Mensaje F: clave de sesión cliente / servidor cifrada con la clave de sesión cliente / TGS.

Pasos de la solicitud de servicio al cliente/ Client Service Request Steps

8. Al recibir los mensajes E y F de TGS, el cliente tiene suficiente información para autenticarse en el SS. El cliente se conecta al SS y envía los dos mensajes siguientes:

A. Mensaje G: compuso el mensaje E recibido del paso anterior (el ticket Cliente a Servidor, cifrado con la clave secreta SS).

B. Mensaje H: un autenticador nuevo, que incluye el ID de cliente, la marca de tiempo y se cifra con Clave de sesión de cliente / servidor.

9. El SS descifra el ticket usando su propia clave secreta para recuperar la Clave de Sesión Cliente / Servidor. Utilizando la clave de sesiones, SS descifra el autenticador y envía el mensaje siguiente al cliente para confirmar su verdadera identidad y su disposición a servir al cliente:

A. Mensaje I: la marca de tiempo que se encuentra en el Autenticador del cliente más 1, cifrada con la clave de sesión Cliente / Servidor.

10. El cliente descifra la confirmación utilizando la clave de sesión de cliente / servidor y comprueba si la marca de hora se actualiza correctamente. Si es así, el cliente puede confiar en el servidor y puede comenzar a emitir peticiones de servicio al servidor.

Conceder acceso

En este punto cada solicitud de servicio para un recurso particular va al SS (Service Server), y se reenvía al procesador RBAC de la ACDU. La ACDU tendrá políticas de

acceso (XML) y almacenadas en la base de datos. Debe tenerse en cuenta que la base de datos de la unidad ACDU está conectada al AS (Authentication Server) para que se puedan obtener las políticas de usuario. El procesador RBAC lee las directivas y se envía a la SS (Service Server) y sobre la base de esta decisión el SS (Service Server) envía un ACK / NACK a la estación del usuario.

B. Publish/ Subscriber Broker

En los sistemas de publicación/ suscripción, los suscriptores proporcionan solicitudes de información al sistema y los editores envían nueva información al sistema. Al recibir una publicación, el sistema busca suscripciones coincidentes y notifica a los suscriptores interesados. Este modelo reduce la complejidad del programa y el consumo de recursos. (Khandakar Entenam Unayes Ahmed, 2014)

En el modelo propuesto el agente de publicación/ subscripción no está directamente conectado al gateway. Los datos recogidos de los sensores irán a **DR (Data Repository)** a través del gateway y la Unidad de Procesamiento de Datos (**DPU**). La **DPU** recortará información innecesaria, formateará la información en un formato de almacenamiento común y enviará los datos al **DR (Data Repository)** para su almacenamiento. Los datos tendrán un índice que será almacenado en el registro del pub/ sub broker. Se utilizará el suscriptor de solicitud **(RS- Request Subscriber)** para crear la suscripción y el identificador de eventos **Event Matcher** (EM) encontrará asignaciones entre las solicitudes de suscripción y los datos publicados. Una vez que se encuentra una asignación, el pub/ sub broker comenzará a buscar datos de la DR (data repository) y canalizará los datos al usuario a través de la interfaz de usuario de la nube. (Khandakar Entenam Unayes Ahmed, 2014)

C. Data Processing Unit

Madden et al., como se citó en (Khandakar Entenam Unayes Ahmed, 2014) explica la propuesta referente a un sistema de procesamiento de consultas de adquisición para redes de sensores, se ilustra la arquitectura básica seguida donde las consultas se envían, analizan, optimizan y se envían a la red de sensores, donde son difundidas y procesadas, con resultados que fluyen de regreso al árbol de enrutamiento que se formó a medida que las consultas se propagaban. Madden desarrolló un modelo adaptativo y sensible al consumo de energía o alimentación para la ejecución de consultas y la recopilación de resultados.

Dos sistemas de almacenamiento de información similares a **Bigtable** denominados **Hbase** e **Hypertable** están construidos sobre el modelo de programación de **Hadoop MapReduce**. **Hypertable** permite que las diferentes columnas lógicas se almacenen físicamente juntas, mientras que **HBase** permite una variación restringida. **HBase** también admite filtros **Bloom** para mejorar las velocidades de acceso. Ambos sistemas de almacenamiento de información proporcionan funcionalidad similar a pesar de tener arquitecturas diferentes. Los datos recogidos se organizan en tablas, filas y columnas. Cada celda se indexa mediante una clave de fila, columna y una marca de tiempo. Varias versiones de la misma fecha se pueden almacenar utilizando marcas de tiempo. Existe una interfaz de tipo iterador que se puede utilizar para escanear columnas. Las envolturas ofrecidas entre ambas tablas y **MapReduce** alientan el desarrollo de nuevas aplicaciones de procesamiento de datos. (Khandakar Entenam Unayes Ahmed, 2014)

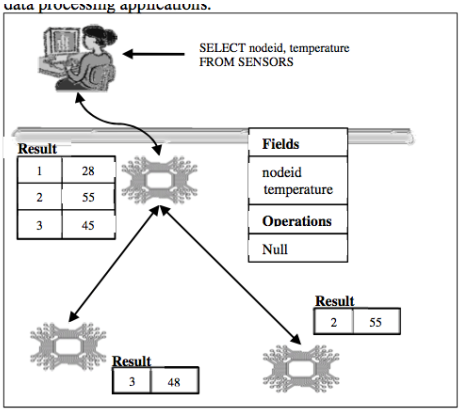


Figura 29. Consulta y resultados que se propagan a través de la red.

Fuente: (Khandakar Entenam Unayes Ahmed, 2014)

El modelo de programación de **MapReduce** sería adecuado para soluciones de bases de datos distribuidas. **MapReduce** puede utilizarse para almacenar y analizar datos de sensores y se ha utilizado en el desarrollo del marco de Cloud Computing propuesto para WSN. (Khandakar Entenam Unayes Ahmed, 2014)

Se ha diseñado un esquema de base de datos para incluir una colección de tablas para almacenar lecturas de sensores individuales y para proporcionar enlaces a lecturas de sensores relacionadas. El modelo propuesto también incluye una metodología para analizar y modelar datos de sensores y varias estadísticas especiales de interés tales como la localización del sensor, el tipo y propósito de la red de sensores, los datos recolectados y otra información global asociada. El modelo propuesto utiliza principios de almacenamiento distribuido y la introducción de **MapReduce** dentro del régimen de almacenamiento de datos permite un mejor almacenamiento y recuperación de datos a través de los sistemas distribuidos. (Khandakar Entenam Unayes Ahmed, 2014)

D. Request Subscriber (RS)

Las solicitudes de servicio se crean sobre la base de la solicitud del usuario para permitir el acceso a los datos almacenados en la **DR (Data Repository)** o para los datos recogidos de una WSN para ser puestos en el **DR (Data Repository)**. Las solicitudes de servicio se pasan a la unidad **RS (Request Subscriber)** que unificará la solicitud y enviará esta solicitud al pub/ sub broker para encontrar una asignación con un índice de datos que se almacena en el registro de broker. (Khandakar Entenam Unayes Ahmed, 2014)

E. Flujo de interacción entre los componentes del modelo

Las interacciones entre los diferentes componentes del modelo propuesto por (Khandakar Entenam Unayes Ahmed, 2014) se muestran a continuación, incluyendo los siguientes pasos:

1. El usuario intenta iniciar sesión enviando información de inicio de sesión.
2. IAMU autenticará al usuario y enviará ACK si la autenticación es correcta.
3. Después de iniciar sesión con éxito, el usuario enviará una solicitud de acceso al servicio.
4. El Cloud Thread (*hilo de ejecución o subproceso de la nube*) identificará el tipo de servicio y generará un mensaje de solicitud correspondiente.
5. Cloud enviará entonces el mensaje de solicitud a Request Subscriber **(RS).**
6. **Request Subscriber RS** unificará la solicitud y creará una suscripción sobre la base de la solicitud recibida del hilo de ejecución de Cloud.
7. Entonces el **Request Subscriber RS** enviará esta suscripción al **PUB / SUB Broker.**

8. **La DPU** (Data Processing Unit) enviará continuamente el índice de los datos **al pub/ sub Broker**. Este evento puede suceder en cualquier momento. Pub/ sub Broker almacenará todos los índices de datos en su registro.

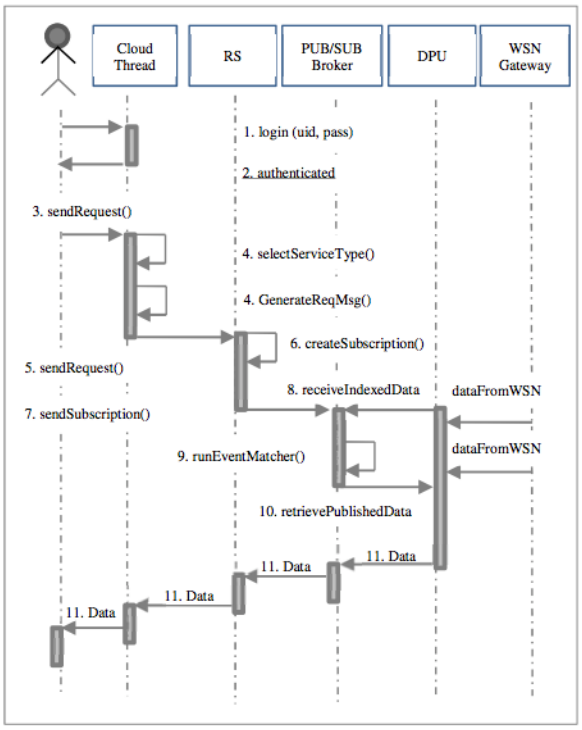


Figura 30. Diagrama de Secuencia- Comunicacion a traves de componentes del modelo.
Fuente: (Khandakar Entenam Unayes Ahmed, 2014)

9. Inmediatamente después de recibir una solicitud de suscripción de **RB (RBAC), parte del ACDU (Access Control Decission Unit) de la IAMU**, **pub/ sub broker iniciará EM (Event Matcher)/ disseminator** para encontrar los datos publicados coincidentes para esta suscripción en particular.

10. Si **Pub/Sub Broker** encuentra cualquier coincidencia de suscripción comenzará a recuperar datos de la **DPU Data Procesing Unit.**

11. Los datos recuperados serán reenviados al usuario a través del **RS (Request Suscriber)** y el hilo de ejecución o subproceso Cloud (Cloud thread).

En referencia al funcionamiento del sistema (Khandakar Entenam Unayes Ahmed, 2014) y (Shah, 2013) explican que los componentes **publisher/ subscriber broker, Request Subscriber, Identity and Access Management Unit (IAMU) and Data Repository (DR).** Los datos recogidos de la WSN son pasados a través del Gateway al PDU, el cual procesa datos y agrega esto al DR (Data Repository). Con el fin de acceder a los datos almacenados de los servicios cloud, los usuarios se conectan a través de la seguridad IAMU (**Identity and Access Management Unit**), en un establecimiento de conexión exitoso el usuario podrá tener el acceso de acuerdo a las políticas de la cuenta. La solicitud de datos del usuario es enviada al **RS (Request Subscriber),** el cual crea una solicitud de suscripción y envía la subscripción al **Pub/ Sub Broker.** Cuando el **PDU (Data Processing Unit)** recibe los datos del Gateway, este envía los datos al **Pub/Sub Broker.** Cuando el evento coincide con la subscripción, los datos son disponibles a los respectivos usuarios. Tiene que haber manera eficaz para el usuario para acceder a los datos obtenidos por los sensores.

2.5.13 Componentes del modelo sensor cloud para permitir colaboración dinámica

(Hassan, 2009) explica que para permitir la colaboración dinámica basada en VO (virtual organization) de proveedores cloud primarios con otros proveedores cloud en caso de violaciones del acuerdo de nivel de servicio (SLA) para la demanda de recursos ráfaga se propone incluir los siguientes componentes:

- **Mediador**:

El mediador (de recursos) es una entidad impulsada por políticas dentro de una VO (Virtual Organization) para asegurar que las entidades participantes sean capaces de adaptarse a las circunstancias cambiantes y sean capaces de alcanzar sus objetivos en un entorno dinámico e incierto. Una vez que se establece un VO (Virtual

Organization), el mediador controla qué recursos se utilizarán de los CLP colaboradores, cómo se toma esta decisión y qué políticas se están utilizando. Al realizar la colaboración automatizada, el mediador también dirigirá cualquier toma de decisiones durante las negociaciones, la gestión de políticas y la programación (scheduling). Un mediador mantiene las políticas iniciales para la creación de VO (Virtual Organization) y trabaja en conjunto con su Agente Colaborador local (CA) para descubrir recursos externos y negociar con otros CLP (Cloud Provider). **[54].**

- **Policy repository (PR):**

El PR virtualiza todas las políticas dentro de la VO (Organización Virtual). Incluye las políticas del mediador, las políticas de creación de VO junto con las políticas de recursos delegados en el VO como resultado de un acuerdo de colaboración. Estas políticas forman un conjunto de reglas para administrar, administrar (manage), y controlar el acceso a los recursos VO. Proporcionan una forma de gestionar los componentes frente a tecnologías complejas.

- **Agente colaborador (CA):**

El CA (collaborator agent) es un módulo de descubrimiento de recursos basado en políticas para la creación de VO (Organizaciones Virtuales) y es utilizado como un conducto por el **mediador** para intercambiar información de políticas y recursos con otros CLPs. Es utilizado por un CLP principal para descubrir los recursos (externos) de los CLP colaboradores, así como para informarles sobre las políticas locales y los requisitos de servicio antes de comenzar la negociación real por el mediador.

Estos componentes actúan colectivamente como un gateway para un CLP (cloud

provider) dado en la formación de una nueva VO (Organización Virtual).

2.5.14 Organización virtual basada en colaboración dinámica

Según (Hassan, 2009) una Organización Virtual VO puede variar en términos de propósito, alcance, tamaño y duración. Por lo tanto, las Organizaciones Virtuales VOs son de dos tipos: VOs a corto plazo bajo demanda (on demand) y VOs a largo plazo con Acuerdos de Nivel de Servicio (SLAs) establecidos. En una Organización Virtual VO a largo plazo, los CLP (Proveedores Cloud) colaboran durante un período más largo de tiempo y tal Organización Virtual (VO) permanece durante todo el evento. En esta situación, esperamos que la negociación incluya un human-directed agent para asegurar que las decisiones resultantes cumplan con las metas u objetivos estratégicos de las empresas participantes. Con el fin de mantener el SLA (acuerdo de nivel de servicio) para cumplir con sus obligaciones de QoS, proponemos que los acuerdos de tiempo crítico para una Organización Virtual (VO) de corto plazo deben negociarse automáticamente. El escenario de formación de una Organización Virtual (VO) se explica en la Figura 31. En la Figura 32 se muestran los pasos de creación de una Organización Virtual VO que se explican de la siguiente manera:

Paso 1: Un proveedor de cloud CLP (principal) se da cuenta de que no puede manejar una parte de la carga de trabajo en su (s) servidor (es) Web. Se envía una solicitud de inicialización de Organización Virtual VO al Mediador.

Paso 2 y Paso 3: La instancia mediadora obtiene el recurso y accede a la información desde el **SR (Service Registry).**

Paso 4: La instancia de **Mediador** en nombre del Cloud Provider CLP principal genera sus requisitos de servicio basados en los requisitos actuales de circunstancia y el SLA

(Acuerdo de Nivel de Servicio) de sus clientes y pasa los requisitos de servicio al **agente colaborador** local (CA).

Paso 5 y Paso 6: Si hay algún arreglo de colaboración preexistente (para un escenario a largo plazo) entonces estos serán devueltos en este punto. De lo contrario, lleva a cabo negociaciones a corto plazo con las CAs (Collaborator Agents) de otros Cloud Provider CLP.

Paso 7: Los SLAs y políticas de otras CAs (Collaborator Agents) se envían a la instancia mediadora (mediator).

Paso 8 y Paso 9: La instancia mediadora (mediator instance) consulta con el repositorio de políticas principal y descubre los mejores colaboradores de Cloud Provider CLP.

Paso 10: La instancia de mediador (mediator instance) solicita una nueva creación de Organización Virtual VO a (Collaborator Agent) CA primaria.

Paso 11: Cuando Collaborator Agent CA primaria adquiere recursos de otros Cloud Providers CLPs colaboradores que cumplen su SLA con los clientes, la nueva Organización Virtual VO se vuelve operativa. Si ningún Cloud Provider CLP está interesado en tal peering, la creación de organización Virtual VO mediante la renegociación se reanuda desde el Paso 4 con requisitos de servicio reconsiderados.

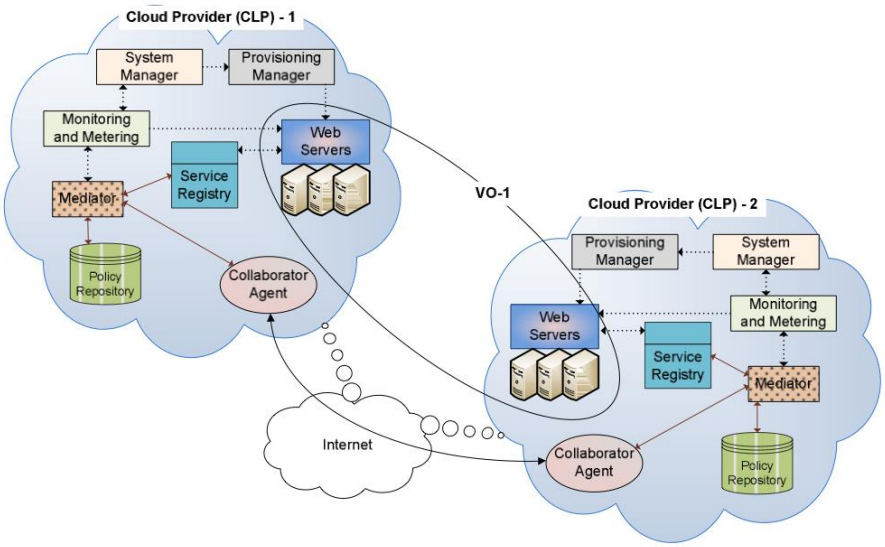


Figura 31. Arquitectura asistida de formación entre VO dinámica y CLP

Fuente: (Hassan, 2009)

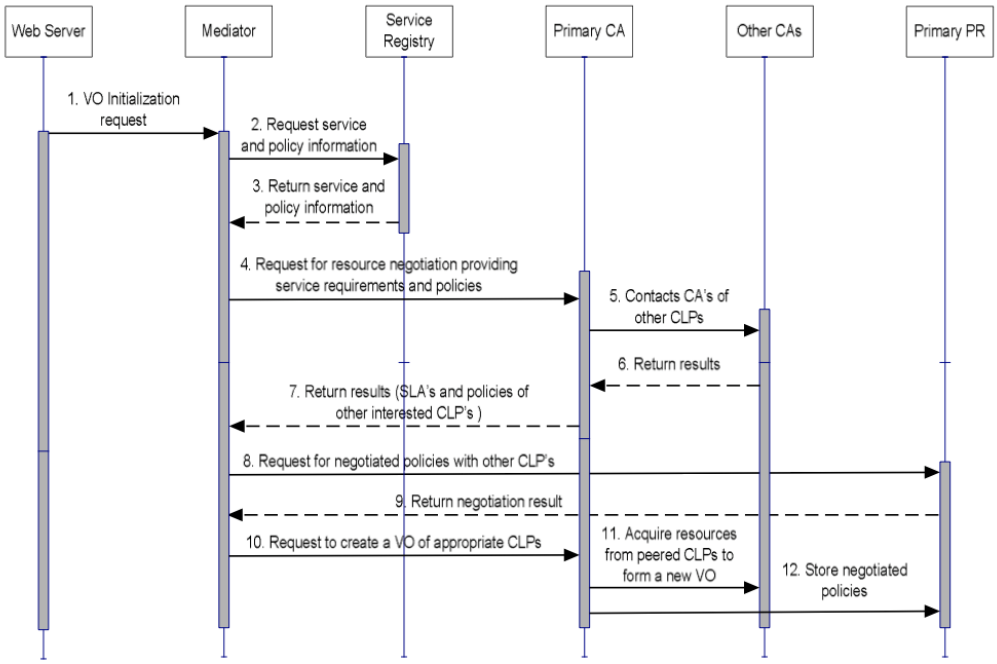


Figura 32. Diagrama de secuencia de formaciòn de una nueva VO

Fuente: (Hassan, 2009)

Pero hay serios problemas involucrados en tales acuerdos, incluyendo la confianza y la potencial sensibilidad comercial de la información sobre el estado actual y los costos de un Cloud Provider CLP. Una solución a estos problemas consiste en utilizar una subasta

criptográficamente segura, que oculta tanto las valoraciones que los Cloud Providers CLP ponen sobre sus recursos como las que participan en la subasta. (Hassan, 2009)

2.5.15 Virtualización en sensor-cloud

Según (K.Lakshmanarao, 2013), una red de sensores se compone de un gran número de nodos de sensores que están densamente desplegados para supervisar una región y obtener datos sobre el entorno. La virtualización de WSN evita el tiempo de inactividad de los nodos sensores físicos y se utiliza para la utilización eficaz de los nodos de sensores físicos al evitar el tiempo de inactividad del nodo sensor físico.

2.5.16 Seguridad en sensor cloud

En referencia a los problemas de seguridad que pueden presentarse en aplicaciones basadas en la información en la arquitectura de computación en la nube, (Guerrero, 2013) explica que un ataque a la seguridad puede surgir dentro de la red, como el cambio del nodo de destino, ruta de enrutamiento inconsistente, información de datos de la escucha, manipulación de datos, ataque de repetición, etc. Cualquier tipo de acceso no autorizado a los datos obstaculizará la seguridad del sistema**.**

Por lo general los datos del conductor se deben almacenar, transmitir y acceder de forma segura. La solución de seguridad debe incluir medidas que permitan seguridad, privacidad y autorización para acceder a los registros de los conductores**.**

2.5.16.1 La confidencialidad y el control de acceso

(Guerrero, 2013) explica que el objetivo principal es proteger la información de su divulgación a terceros no autorizados. El componente clave de la protección de

confidencialidad de la información se podría lograr mediante la adopción de la técnica de cifrado/ descifrado. Los métodos de autenticación y autorización será garantizar el acceso a los datos sólo los usuarios legítimos. El método de cifrado/ descifrado usando criptografía de clave simétrica como AES es más adecuado para proporcionar confidencialidad de los datos. El proceso de autenticación incluye la identificación del usuario y la validación generalmente se logra usando credenciales como combinación de ID de usuario y la contraseña, número de pin, etc.

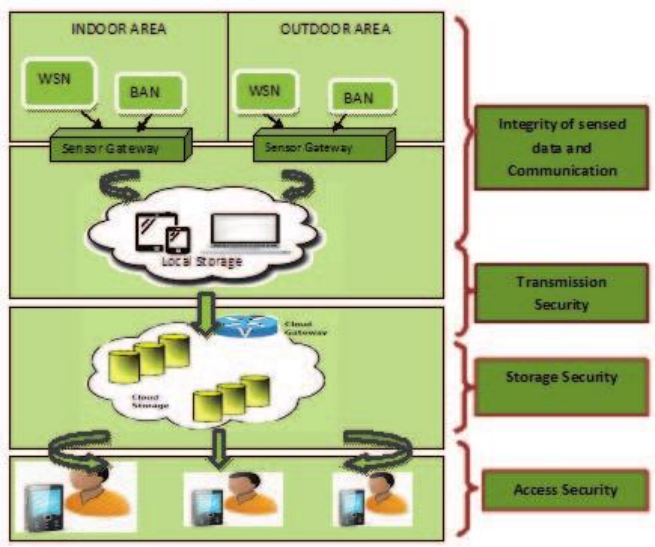


Figura 33. Modelo de solución de seguridad para aplicaciones basadas en el entorno de integración sensor cloud.
Fuente: (Guerrero, 2013)

2.5.16.2 Integridad

La integridad de la información se refiere a la protección de la información de la manipulación por personas no autorizadas. Esta propiedad asegura la precisión y consistencia de los datos. Comúnmente métodos utilizados para proteger la integridad de datos incluyen el hash de los datos recibidos y compararlo con el hash del mensaje/ datos originales. Sin embargo, esto significa que el hash de los datos originales se debe

proporcionar de una manera segura. Las variantes del algoritmo de hash seguro como SHA-224, SHA-256, SHA-384 y SHA-512 pueden servir para este propósito. (Guerrero, 2013)

2.5.16.3 Disponibilidad

La disponibilidad de información se refiere a garantizar que las personas autorizadas puedan acceder a la información cuando sea necesario. Los servicios de cloud computing ya soportan datos de copia de seguridad y técnica de redundancia para mantener múltiples copias de datos de manera que el punto único de fallo podría evitarse y los datos siempre estan disponibles. (Guerrero, 2013)

2.5.17 Aplicaciones de sensor cloud

(Wasai Shadab Ansari, 2012) explica las siguientes aplicaciones para la infraestructura sensor cloud:

2.5.17.1Salud ubicua

Los sensores como sensores de calor, sensores de cama, estufa de sensor, cámara y los sensores de acelerómetro, etc se pueden utilizar juntos en la supervisión de los residentes de edad muy avanzada para prevenir de cualquier siniestro sin ser dañado e interrumpiendo ellos. Estos servicios sensores pueden proporcionar la percepción de los residentes de edad avanzada en los servicios de salud.

2.5.17.2 Monitoreo Ambiental para la detección de emergencias/ desastres

En aplicaciones ambientales puede ser utilizado para detectar un terremoto y explosión volcánica antes de su erupción supervisa de forma continua a través del uso de varios números de diferentes sensores como la tensión, temperatura, luz, imagen, sonido,

aceleración, sensores de barómetro etc mediante el uso de Las redes de sensores inalámbricos.

2.5.17.3 Telemática:

Sensor cloud se puede utilizar para la telemática de medios para implementar la transmisión a larga distancia de nuestra información a un sistema en continuo. Permite la comunicación fluida entre el sistema y los dispositivos sin ninguna intervención.

2.5.17.4Google Health:

Es un servicio de centralización de Google que proporciona información personal de salud y sirve como almacenamiento de datos de la nube de salud. A los usuarios de Google se les permite controlar sus registros de salud al iniciar sesión en sus cuentas de proveedores de servicios cloud de salud colaborado en el sistema de salud de Google.

2.5.17.5 Microsoft Health Vault:

Esta plataforma en la nube es desarrollada por Microsoft para almacenar y mantener la salud y relacionada con la información de forma física. Salud-Vault ayuda a los usuarios a almacenar, se reúnen y comparten su información relevante de salud y estos datos pueden ser adquiridos en varias farmacias, proveedores de nube, empleados de salud, laboratorios, equipos de salud y de los propios usuarios.

2.5.17.6 Agricultura y control de riego

Sensor de la nube puede ser utilizado en el campo de la agricultura para controlar los campos de cultivo con el fin de que el mantenimiento. Para ello se desarrolló un servidor de campo que comprende unos sensores de cámara, el sensor de aire, sensores de temperatura, sensores de concentración de CO2, humedad del suelo y sensores de temperatura etc. Estos sensores cargar continuamente los datos de campo a través de

punto de acceso Wi-Fi para el propietario de campo para realizar un seguimiento la salud de sus cultivos. Esto también puede ser utilizado para la cosecha.

2.5.17.7 Observación de la Tierra

Una red de sensores se ha desarrollado para la recopilación de datos de varias estaciones de GPS, para procesar, analizar, gestionar y visualizar los datos GPS [39]. Estos datos GPS a continuación, se incluirán en la nube para una supervisión eficaz, la alerta temprana, y la capacidad de toma de decisiones en situaciones críticas, como las erupciones volcánicas, terremotos, tsunamis, ciclones, etc. a los usuarios de todo el mundo.

2.5.17.8 El transporte y el tráfico de vehículos

Sensor cloud puede ser utilizado para proporcionar un servicio eficiente, estable, equilibrado y sistema de seguimiento sostenible. A principios de tecnologías existentes como la navegación GPS sólo puede seguir el estado y la ubicación actual del vehículo, pero cuando ponemos en práctica este vehículo monitoreo utilizando cloud computing, servicio web centralizado, GPS y dispositivos con capacidad GSM, dispositivo integrado con sensores instalados en ella, se activa para identificar el nombre actual de la ubicación, predecir el tiempo de llegada, identificar el estado del conductor a través del sensor de alcohol en el aliento, encontrar la distancia total cubierta y realizar un seguimiento del nivel de combustible; todos los datos captados se almacenan en algún servidor centralizado que reside en la nube. El propietario del vehículo puede acceder a estos datos en la nube a través del portal web y puede recuperar todos los datos en la nube en tiempo real para visualizar la información del vehículo.

2.5.18 Servicios WEB

El consorcio W3C define los Servicios Web como sistemas software diseñados para soportar una interacción interoperable maquina a maquina sobre una red. Los Servicios Web suelen ser APIs Web que pueden ser accedidas dentro de una red (principalmente Internet) y son ejecutados en el sistema que los aloja. (Navarro, 2006)

La definición de Servicios Web propuesta alberga muchos tipos diferentes de sistemas, pero el caso común de uso se refiere a clientes y servidores que se comunican mediante mensajes XML que siguen el estándar SOAP o REST. (Navarro, 2006)

2.5.18.1Definición REST

REST (Representational State Transfer) es un estilo de arquitectura de software para sistemas hipermedias distribuidos tales como la Web. (Navarro, 2006)

REST se refiere estrictamente a una colección de principios para el diseño de arquitecturas en red. Estos principios resumen como los recursos son definidos y diseccionados. El término frecuentemente es utilizado en el sentido de describir a cualquier interfaz que transmite datos específicos de un domino sobre HTTP sin una capa adicional, como hace SOAP. Estos dos significados pueden chocar o incluso solaparse. Es posible diseñar un sistema software de gran tamaño de acuerdo con la arquitectura propuesta por **Fielding** sin utilizar HTTP o sin interactuar con la Web. Así como también es posible diseñar una simple interfaz XML+HTTP que no sigue los principios REST, y en cambio seguir un modelo RPC. (Saymon Castro de Souza, 2013)

El estilo de arquitectura que se empleará en los servidores WEB de la arquitectura propuesta es REST, esta arquitectura está basada en los estándares: HTTP, URL, XML, HTML, GIF, JPEG, TEXT, HTML. (Navarro, 2006)

Según (Navarro, 2006) entre los objetivos y características principales la arquitectura REST permitirá:

- Escalabilidad de la interacción con los componentes, gracias a lo cual pueden acceder variedad de clientes: estaciones de trabajo, dispositivos móviles.
- Generalidad de interfaces, gracias al protocolo HTTP cualquier cliente puede interactuar con cualquier servidor HTTP.
- Puesta en funcionamiento independiente, es decir, que se adapte a las arquitecturas antiguas.
- Compatibilidad con componentes intermedios, como por ejemplo proxys para web, firewalls y gateways, con el propósito de reducir la latencia de interacción, reforzar la seguridad y encapsular otros sistemas.

Además (Navarro, 2006) explica que el estilo de arquitectura REST maneja las siguientes restricciones:

- **Identificación de recursos y manipulación de ellos a través de representaciones,** lo cual se consigue mediante el uso de URIs, los recursos son objetos lógicos a los que se envían mensajes y no pueden ser directamente accedidos o modificados sino que se trabaja con representaciones de ellos.
- **Mensajes autodescriptivos**, lo cual permite que los intermediarios interpreten los mensajes y ejecuten servicios en nombre del usuario, http logra esto por medio del uso de varios métodos estándar (PUT, GET, POST y DELETE), muchos encabezamientos y un mecanismo de direccionamiento.
- **Hipermedia como un mecanismo del estado de la aplicación,** permite al servidor conocer el estado de sus recursos, ya que el estado actual de una aplicación web es capturada en uno o más documentos de hipertexto.

2.5.18.2 Diseño REST

La Web consiste del protocolo HTTP, de tipos de contenido incluyendo HTML y otras tecnologías tales como el DNS. Cuando se utiliza REST, http no tiene estado, cada mensaje contiene toda la información necesaria para comprender la petición cuando se combina el estado en el recurso, como resultado ni el cliente ni el servidor necesitan mantener ningún estado en la comunicación. Cualquier estado mantenido por el servidor debe ser modelado como un recurso. (Navarro, 2006).

HTTP proporciona mecanismos para el control del caching y permite que ocurra una conversación entre el navegador y la caché del mismo modo que se hace entre el navegador y el servidor web. (Navarro, 2006)

2.5.18.3 Características de REST VS SOAP

(Navarro, 2006) menciona que REST es un sistema potencialmente escalable, además el acceso a sus operaciones es con escaso consumo de recursos debido al limitado número de operaciones y el esquema de direccionamiento unificado. A continuación, en la Tabla 4 se muestra la comparación entre las características, ventajas, protocolos, seguridad y metodologia de diseño de REST vs. SOAP.

TABLA 4. CARACTERÍSTICAS REST VS SOAP

	REST	SOAP
TECNOLOGÍA	Interacción dirigida por el usuario por medio de formularios	Flujo de eventos orquestados
	Pocas operaciones con muchos recursos	Muchas operaciones con pocos recursos
	Mecanismo consistente de nombrado de recursos	Falta de un mecanismo de nombrado
	Se centra en la escalabilidad y rendimiento a gran escala para sistemas distribuidos hipermedia	Se centra en el diseño de aplicaciones distribuidas
PROTOCOLO	XML autodescriptivo	Tipado fuerte, XML Schema
	HTTP	Independiente del transporte
	HTTP es un protocolo de aplicación	HTTP es un protocolo de transporte
	Síncrono	Síncrono y Asíncrono
DESCRIPCIÓN DEL SERVICIO	Confía en documnetos orientados al usuario que define las direcciones de petición y las respuestas	WSDL
	Interactuar con el servicio supone horas de testeado y depuración de URIs	Se pueden construir automáticamente stubs (clientes) por medio del WSDL
	No es necesario el tipado fuerte si ambos lados están de acuerdo con el contenido	Tipado fuerte
	WADL	WSDL 2.0
GESTIÓN DEL ESTADO	El servidor no tiene estado (stateless)	El servidor puede mantener el estado de la conversación
	Los recursos contienen datos y enlaces representando transiciones a estados válidos	Los mensajes solo contienen datos
	Los clientes mantienen el estado siguiendo los enlaces	Los clientes mantienen el estado suponiendo el estado del servicio
	Técnicas para añadir sesiones: cookies	Técnicas para añadir sesiones: Cabecera de sesión (no estándar)
SEGURIDAD	HTTPS	WS-Security
	Implementado desde hace muchos años	Las implementaciones están empezando a aparecer
	Comunicación punto a punto segura	Comunicación origen a destino segura
METODOLOGÍA DE DISEÑO	Identificar recursos a ser expuestos como servicios	Listar las operaciones del servicio en el documento WSDL
	Definir URLs para direccionarlos	Definir un modelo de datos para el contenido de los mensajes

	Distinguir los recursos de solo lectura (GET) de los modificables (POST, PUT, DELETE)	Elegir un protocolo de transporte apropiado y definir las correspondientes políticas QoS, de seguridad y transaccional
	Implementar e implantar el servidor Web	Implementar e implantar el contenedor del servicio Web

Fuente: (Navarro, 2006)

CAPITULO III:

ANÁLISIS COMPARATIVO DE TECNOLOGÍAS UTILIZADAS EN APLICACIONES VEHICULARES

Este capítulo abarca la comparación de los estándares GPRS y VANET con la tecnología SENSOR CLOUD, se explican sus características técnicas y el tipo de aplicaciones a las que están orientadas. Además se analiza el comportamiento de estos sistemas frente a una aplicación de monitoreo vehicular similar a la propuesta en este proyecto.

Esto permite establecer si en el mercado estas tecnologías serán competidoras ante una misma aplicación o si de lo contrario serán estándares complementarios, que podrán convivir en un ambiente de trabajo común.

3.1Tecnología GPRS (sistema general de paquetes vía radio)

3.1.1 Definición

Según (Juan G. Tamayo, 2013) al sistema GPRS se le conoce también como GSM-IP ya que usa la tecnología IP (Internet Protocol) para acceder directamente a los proveedores de contenidos de Internet.

La tecnología GPRS comparte el rango de frecuencias de la red GSM utilizando una transmisión de datos por medio de paquetes, es decir, usa el procedimiento de conmutación de paquetes. Nace como la evolución de la actual red GSM, reutiliza su misma infraestructura, lo que no conlleva a grandes inversiones y mantiene su misma cobertura. (Juan G. Tamayo, 2013)

3.1.2 Funcionamiento

GPRS utiliza la red de telefonía celular solo cuando los datos son enviados o recibidos. Mediante el protocolo IP los datos se dividen en fragmentos que se envían separadamente por la Red, reconstruyéndose al llegar a su destino, esto optimiza la utilización del espectro de radio disponible, ya que no es necesario que un canal sea utilizado exclusivamente para la transmisión de un punto a otro. La utilización en las redes móviles del mismo protocolo de transmisión de datos que en Internet, permitirá que todos los servicios en línea estén disponibles en el terminal móvil. Cada móvil podrá tener su propia dirección IP, como cualquier terminal conectado a Internet, y será identificado en la Red por este número. (Juan G. Tamayo, 2013)

Para el caso concreto de transmitir datos a grandes distancias, la Tecnología GPRS es la que presenta mayores ventajas debido a la flexibilidad, escalabilidad y al reducido costo de la misma, por tal razón desde el punto de vista económico esta tecnología es la más adecuada.

3.1.3 Características

(Guerrero, 2013) y (Juan G. Tamayo, 2013) explican las siguientes características:

- GPRS permite a los usuarios móviles enviar y recibir datos en forma de paquete a través de protocolos como: TCP/IP, UDP (Protocolo de Transporte sin Conexión), X.25, y CLNP1 (Protocolo de Red sin Conexión)
- GPRS ofrece acceso a redes de datos estándar.
- **Conexión permanente "Always On":.-** El tiempo de establecimiento de la conexión es prácticamente instantáneo, por lo que el usuario percibe que está siempre conectado.

- **Mayor velocidad de transmisión:** GSM utiliza un canal dedicado (un timeslot), a una velocidad máxima de 9.6 Kbps. Con GPRS se tiene varios canales asignados, con lo que la velocidad de transmisión de datos aumenta desde un mínimo de 21.4 Kbps y un máximo de 144 Kbps por comunicación.
- **Facturación**: No se realiza por establecimiento o tiempo de conexión sino por volumen de información intercambiada. Costo nulo de establecimiento de la transmisión.
- **Eficiencia**: Los canales de comunicación se comparten entre los usuarios dinámicamente, de modo que un usuario sólo tiene asignado un canal cuando está realmente transmitiendo datos. Logrando de esta manera el uso más eficiente de los recursos de la red y del espectro radioeléctrico, puesto que comparte el rango de frecuencias de la red GSM.
- **Modo de transmisión asimétrico**: Adaptado al tipo de tráfico de navegación html o wml. Si un terminal es de tipo GPRS 4+1; quiere decir que el terminal tiene capacidad de 4 slots en el enlace downlink y 1 slot en el enlace uplink, por tanto tendrá cuatro veces mayor capacidad de transmisión de bajada que de subida.
- **La posibilidad de realizar y recibir llamadas de voz mientras se esté conectando o utilizando cualquiera de los servicios disponibles con GPRS**. Según el terminal que se utilice se puede asignar calidades de servicio (QoS) diferenciadas a los distintos usuarios móviles.
- **La tecnología de paquetes le permite separar las asignaciones de recursos** entre enlace ascendente y descendente.

3.1.4 Arquitectura de la red GPRS

En cuanto a la arquitectura de la red GSM/GPRS, (Guerrero, 2013) define entidades

funcionales agrupadas en subsistemas:

- Subsistema de Estación Base (BSS) (*Base Station Subsystem*)
- Subsistema de Conmutación de Red (NSS) (*Network Switching Subsystem*)
- Subsistema de estación móvil (MSS) (*Mobile Station Subsystem*)
- Subsistema de operación y mantenimiento (NMS) (*Network Management Subsystem*).

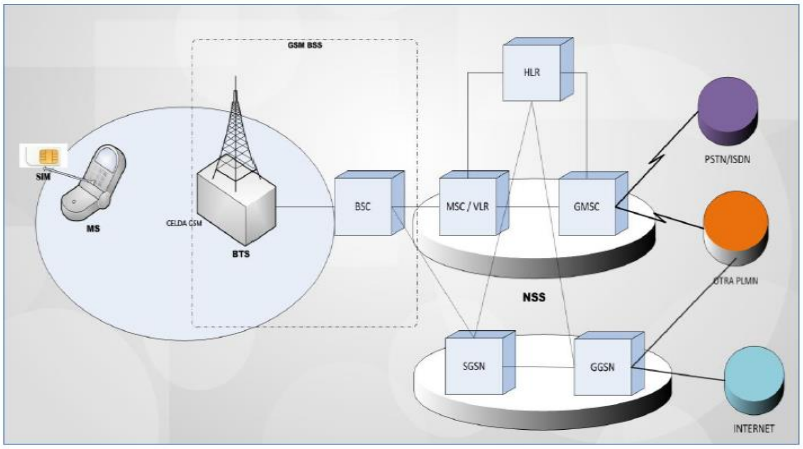


Figura 34. Elementos que agrega GPRS

Fuente: (Juan Carlos Amay Izquierdo, 2014)

La red GPRS agrega algunos componentes a la red GSM tales como el **SGSN** (Serving GPRS Support Node) (responsable de la transferencia de paquetes) y el **GGSN** (Gateway GPRS Support Node) (convierte los paquetes al formato IP) que no estaban incluidos en un principio en la red GSM. La inclusión de estos nuevos componentes permite la conmutación de paquetes y la utilización de protocolos IP. (Juan Carlos Amay Izquierdo, 2014)

La estructura de GSM se ha modificado hasta encontrar un modo de transferencia de conmutación de paquetes de extremo a extremo y los encargados de esta función son

los nodos de soporte del servicio denominados GSN (Gateway Support Node). (Juan Carlos Amay Izquierdo, 2014)

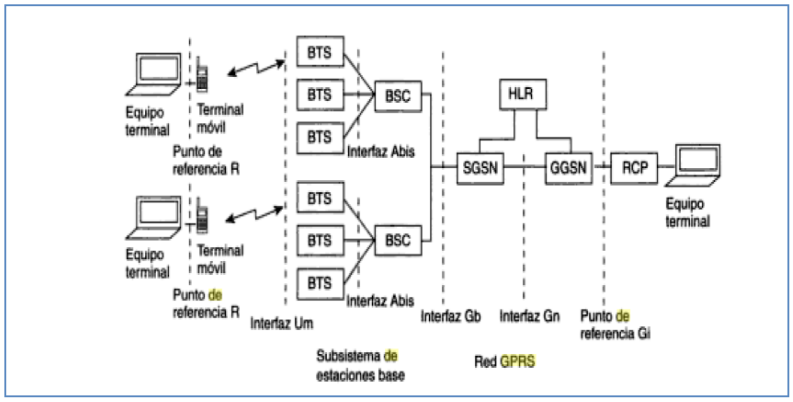


Figura 35. Arquitectura del sistema GPRS.
Fuente: (Juan Carlos Amay Izquierdo, 2014)

(Juan Carlos Amay Izquierdo, 2014), describe los elementos que ayudan a encaminar los paquetes de datos desde y hacia las estaciones móviles:

- **SGSN**.- Nodo de soporte servidor GPRS (Serving GPRS Support Node), responsable de la transferencia de los paquetes desde y hacia los móviles en su área de servicio. Gestiona la movilidad, la autenticación y cifrado. Así como también se encarga de recopilar toda la información necesaria para la facturación.
- **GGSN**.- Nodo de soporte de pasarela de GPRS (Gateway GPRS Support Node), actúa como interfaz lógica entre la red GPRS y las redes públicas de datos (PDN) externas que pueden ser IP o X25.

Tanto el SGSN y GGSN son parte del GSN. Todos los nodos GGSN se conectan a través de una troncal GPRS (backbone network) basada en IP. Se diferencian dos clases de troncales: Intra-PLMN GPRS Backbone (Red Troncal GPRS) e Inter-PLMN GPRS Backbone (Inter Operator GPRS). Como podemos observar en la Figura 36 la

troncal Intra-PLMN permite la conexión entre los GSN de una misma operadora. Mientras que la Inter-PLMN servirá para conectar redes troncales GPRS o Intra PLMN de distintas operadoras.

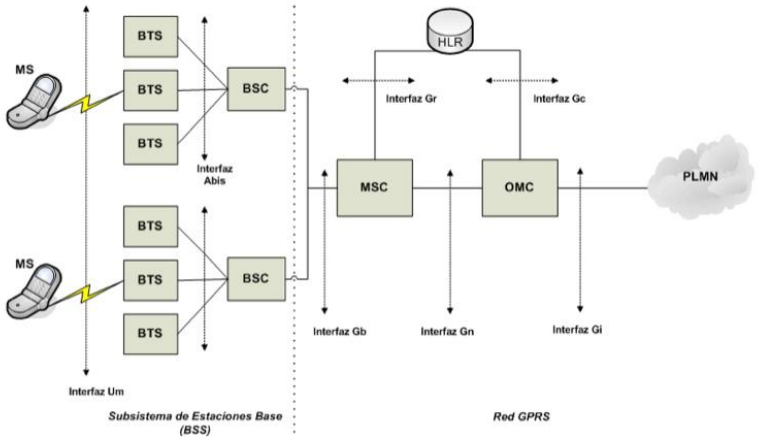


Figura 36. Arquitectura GPRS

Fuente: (Juan Carlos Amay Izquierdo, 2014)

3.1.5 Interfaces de red GPRS

Según (Guerrero, 2013) y (Sánchez, 2005) a continuación se mencionan las interfaces de la red GPRS:

- **Interfaz Gn.**
  - Se encarga de la transmisión de información entre el SGSN y el GGSN.
  - Opera el GTP (GPRS Tunnel Protocol), que usa el mecanismo de "tunneling" entre los GPRS Support Nodes en la red backbone GPRS, también se trabaja con los protocolos TCP/UDP e IP.
- **Interfaz Gi.**
  - Tiene la finalidad de comunicar a la red GPRS con las redes exteriores.

- **Interfaz Gb.**
  - Esta interfaz, se encarga de establecer todo el dialogo con el terminal móvil.

- **Interfaz Gs.**
  - Se utiliza entre el MSC/Registro de Lugares Visitantes (RLV) y el SGSN para coordinar el envío de señales para terminales móviles capaces de manejar datos por conmutación de circuitos y por paquetes.

3.1.6 Ventajas y desventajas de la red GPRS

Según (Guerrero, 2013) y (Fernando Paúl Espinoza Peñaherrera, 2009) a continuación se mencionan las ventajas y desventajas de la red GPRS:

3.1.6.1 Ventajas

- General Packet Radio Service o GPRS es una tecnología digital de telefonía móvil.
- GPRS básicamente es una comunicación basada en paquetes de datos. Los timeslots (intervalos de tiempo) se asignan a la conexión de paquetes mediante un sistema basado en la necesidad. Esto significa que si no se envía ningún dato por el usuario, las frecuencias quedan libres para ser utilizadas por otros usuarios.
- La tecnología GPRS permite proporcionar servicios de datos de una forma más eficiente.
- Mejora sustancialmente el sistema de mensajería, permitiendo Multimedia Messagging Subsystem (MMS) con mensajes de voz, texto, imágenes y video.
- Cuatro niveles de codificación radio.
- Cada elemento de la red sabe cómo encaminar cada paquete.
- Obtiene mayor velocidad y mejor eficiencia de la red.
- GPRS provee un mejor ancho de banda para las comunicaciones de datos.

- La facturación se realiza por volumen de datos transmitidos y no en función del tiempo de conexión, lo que representa ahorro ya que sólo se pagará por el uso efectivo que se haga de la red.
- GPRS da la posibilidad de realizar o recibir llamadas de voz cuando se está conectado o utilizando los demás servicios que brinda esta tecnología, lo cual se logra separando el canal de datos con el canal de voz de esta forma permite el uso de ambos canales sin que interfieran entre ellos.
- GPRS es la evolución de las redes GSM, cuyo objetivo es proporcionar mayores velocidades y mejores prestaciones en el acceso móvil a los servicios de datos e internet. GPRS reutiliza parte de la infraestructura actual de GSM, es decir complementa a estas redes, no las sustituye.
- La tecnología GPRS comparte cada canal con varios usuarios, de esta forma mejora la eficiencia del uso de los recursos de la red.

3.1.6.2 Desventajas

- Existen colas de espera en cada nodo, lo que da un cierto retardo, el mismo que es mayor que en conmutación de circuitos.
- La posibilidad de congestión, debido a que la red acepta paquetes más allá del límite que tiene para despacharlos.

3.1.7 Protocolos

3.1.7.1 Protocolo GPRS

Según (Sánchez, 2005) es un protocolo de nivel tres, soporta tanto el intercambio de informaciones de control como de paquetes PDP-PDU (Packet Data Protocol - Protocol

Data Unit) entre el móvil y el nodo al que este está conectado (los PDP-PDU son encapsulados en las tramas GPRS).

3.1.7.2 Formato de trama GPRS

La trama GPRS según explica (Guerrero, 2013) y (Sánchez, 2005) tiene los siguientes campos:

- **Identificador del protocolo GPRS.-** es un dato numérico cuyo objetivo es distinguir las ráfagas (burst) que contienen paquetes GPRS, de los que contienen información GSM.
- **Identificador del protocolo de los PDU (identificador de PDP).-** encapsulados en las tramas GPRS, dicha información permite la interpretación del GPRS contenido en la trama GPRS; Las tramas GPRS son utilizadas tanto para el transporte de mensaje de control como para el de paquetes de datos, por tal razón es necesario el uso de un indicador que reconozca a cuál de las dos categorías posibles pertenece el mensaje GPRS.
- **Mensaje GPRS.-** de control son definidos por un valor pre establecido del identificador de PDP.

3.1.8 Aplicación de GPRS en un sistema de rastreo vehicular

En la investigación (Guerrero, 2013) se explica una aplicación basada en el rastreo por medio de GPRS, el cual permite la comunicación para el envío de coordenadas del equipo móvil, eventos, y configuraciones hacia un servidor en el cual se encuentra una aplicación o sistema web, esta transmisión es a través de redes externas como es el caso del internet, la comunicación se ejecuta mediante el protocolo TCP/IP.

Se presenta un diagrama de los procesos a ejecutarse para el funcionamiento y el propósito del requerimiento a obtenerse.

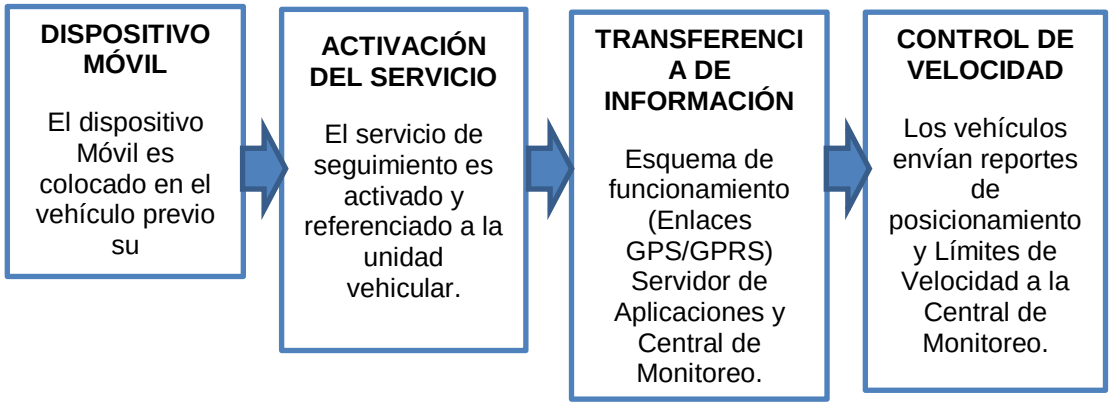


Figura 37. Diagrama de los procesos a ejecutarse para el funcionamiento de una aplicación GPRS

Fuente: (Guerrero, 2013)

- El principio básico del sistema de rastreo es la utilización de satélites para las señales GPS, las mismas que son transmitidas a los equipos de rastreo, una vez que los equipos GPS reciben la señal satelital, estos pueden trasmitir la información en tiempo real, mediante una red GSM o servicio general de paquetes vía radio (GPRS) a una plataforma de rastreo, para realizar un monitoreo de la ubicación y el control de velocidad de unidades vehiculares.
- Mediante la red GPRS se envía la información del vehículo.
- El equipo hardware instalado en el vehículo recibe la información de los satélites GPS y transmite la información a los servidores de aplicación y monitoreo mediante la red celular (GPRS), luego se procesa esta información para la disposición del cliente.
- Respecto al almacenamiento tiene que ser tipo hardware en el servidor de almacenamiento de la central de monitoreo.

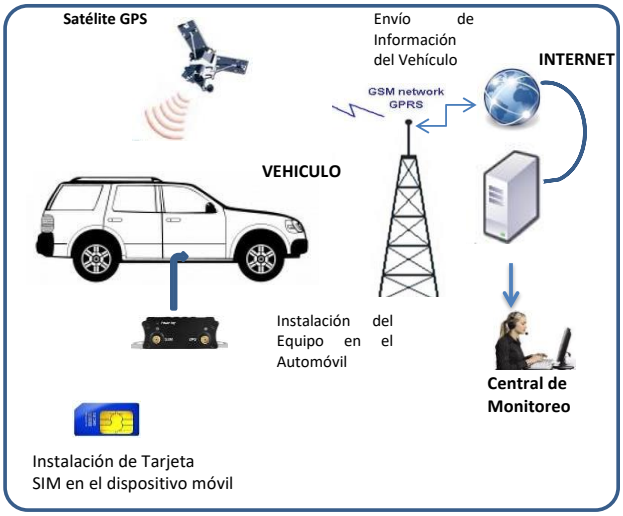


Figura 38. RED GSM /GPRS y hardware a utilizar

Fuente: (Guerrero, 2013)

3.1.9 Transmisión de información a través de la red GPRS

- **Activación del equipo.-** El chip debe estar activado con algún plan de datos de preferencia (para enviar información al centro de monitoreo)

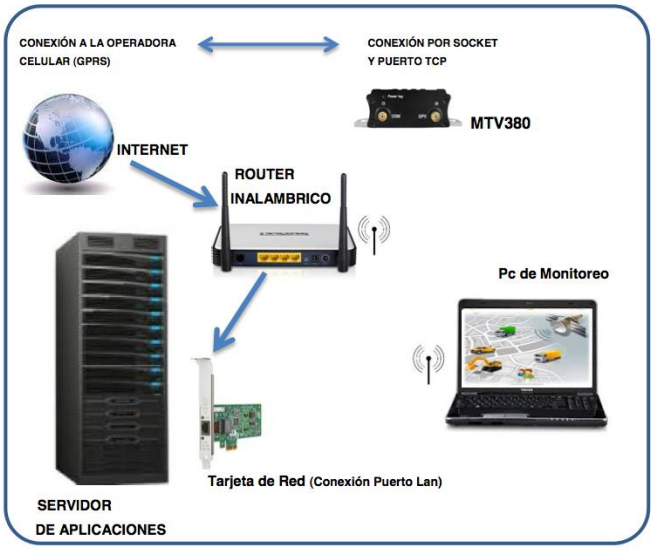


Figura 39. Aplicación de monitoreo

Fuente: (Guerrero, 2013)

- **RASTREO POR MEDIO DE GPRS.-** El dispositivo envía las coordenadas y los eventos por medio del internet (GPRS), para que por medio de un aplicativo web reciba la información el servidor.

3.1.10 Seguridad de la información en GPRS

En referencia a los temas de seguridad de GPRS, (Guerrero, 2013) menciona lo siguiente:

- Seguridad física.
- Seguridad lógica.
- Tecnologías de seguridad.- Se puede aplicar diversos mecanismos para la seguridad como el uso de algoritmos de encriptación y aplicándolos en los distintos niveles del TCP/IP, en las diferentes capas del modelo.

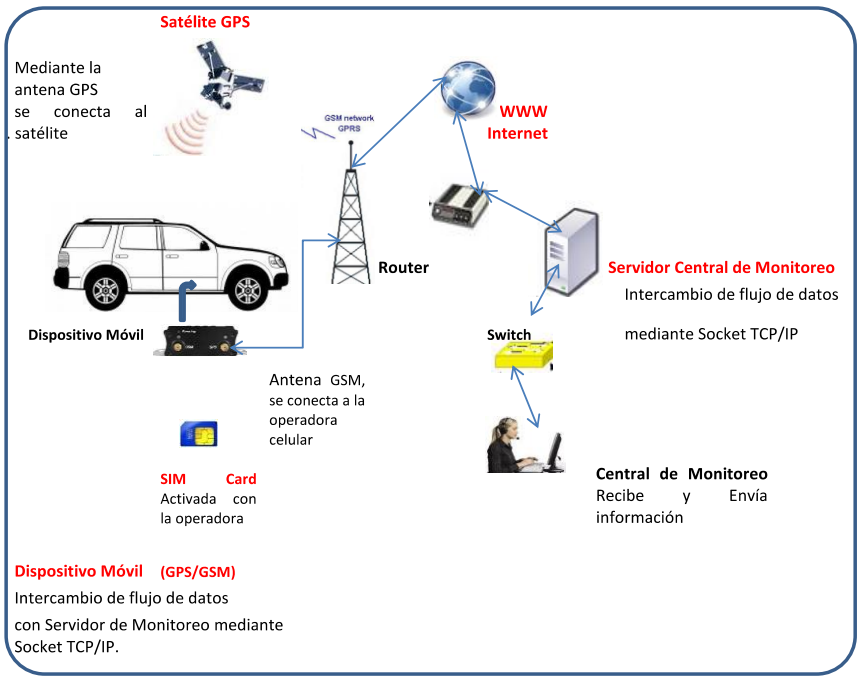


Figura 40. Diagrama de las conexiones para el envío y recepción de la información entre equipos

Fuente: (Guerrero, 2013)

3.1.11 Conexión de GPRS al internet

Se conecta a través de la MSC (Central Intercambiadora de Servicios Móviles), que es una central de conmutación encargada de todas las funciones de conmutación para las estaciones móviles, y proporciona conexión con otras redes. (Tello, 2012)

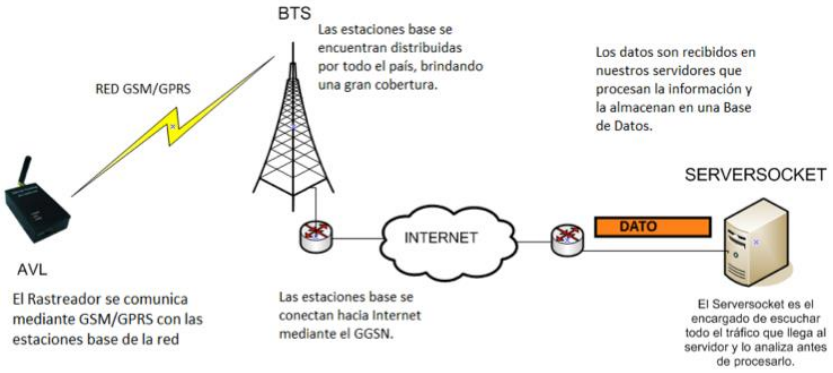


Figura 41.Conexión de GPRS a internet. Serversocket

Fuente: (Tello, 2012)

Las estaciones base se conectan hacia el internet mediante el GGSN

3.1.12 Aplicaciones

Según (Donato, 2010) algunos ejemplos de aplicaciones que cumplen esas características son:

- RTI (Road Traffic Informatics)
- Telemetría
- Telealarma
- Control del tráfico ferroviario
- Acceso a internet usando la www (World Wide Web)

3.2 Redes vehiculares VANETS

3.2.1 Definición

(Víctor Sandonís Consuegra, 2014), define las redes vehiculares o Vehicular Ad hoc Networks (VANETs) como la tecnología más apropiada para proporcionar a los vehículos capacidades de comunicación que se pueden aplicar a la mejora de la seguridad vial, mejora de la eficiencia del tráfico en carreteras y áreas urbandas. Las VANETs también abren la puerta del mercado a aplicaciones no relacionadas con la seguridad vial entre las que destaca la conectividad a Internet.

Una red vehicular o Vehicular Ad hoc Network (VANET) es una red ad hoc formada por vehículos equipados con interfaces inalámbricas que pueden comunicarse entre sı de manera descentralizada de forma que los vehículos reciben y reenvían los paquetes de datos procedentes de otros nodos de la red. Las VANETs permiten a los vehículos el establecimiento de comunicaciones para el intercambio de información donde se puede diferenciar entre comunicaciones Vehicle-to-Vehicle (V2V) y comunicaciones Vehicle-to-Infrastructure (V2I). (Víctor Sandonís Consuegra, 2014)

Una red vehicular o VANET es una red ad hoc en la que los nodos de la red son vehículos y por lo tanto, se encuentran en movimiento. De esta manera, las VANETs son un caso particular de las denominadas redes ad hoc móviles o MANETs (Mobile Ad hoc NETworks). Lo que diferencia a las VANETs de otro tipo de redes ad hoc móviles es que sus nodos pueden moverse a una gran velocidad, y por lo general, siguiendo un patrón restringido. Es decir, los vehículos se mueven sobre carreteras con una determinada topología y respetando unas normas de circulación. Una característica muy importante de las redes vehiculares es que la elevada movilidad de los vehículos hace que los enlaces entre ellos sean muy inestables para las comunicaciones. Además, los vehículos pueden contar con grandes capacidades de memoria y

procesamiento. En cambio, en otros tipos de MANETs, los nodos pueden seguir un patrón de movilidad arbitrario y la capacidad de memoria y computación pueden estar limitadas. (Víctor Sandonís Consuegra, 2014)

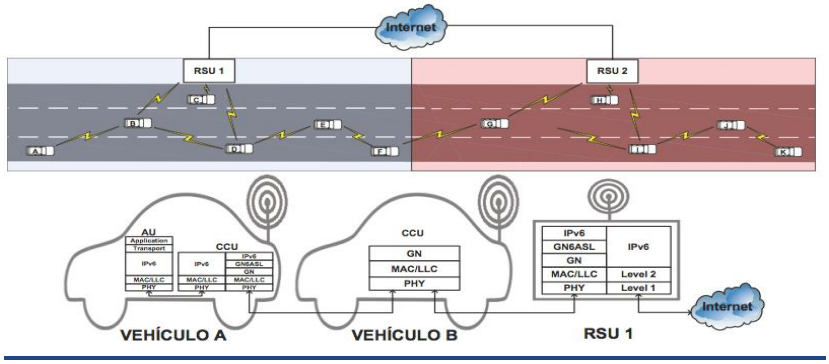


Figura 42. Arquitectura VANET

Fuente: (Víctor Sandonís Consuegra, 2014)

Las Redes VANETs o Redes Ad-Hoc, no son más que Redes enfocadas a entornos vehiculares, en las cuales sus nodos son vehículos (automóviles, camiones, buses, etc.) los cuales constituyen una Red en pleno movimiento. Los nodos se mueven en forma arbitraria y pueden comunicarse entre ellos o pueden tener comunicación con algún tipo de infraestructura (ICESI, 2010). Estas Redes se crean de forma espontánea, con el movimiento de vehículos equipados con interfaces inalámbricas ***(OBUs - On Board Unit),*** que les permiten comunicarse unos con otros. De no ser posible la comunicación directa entre dos vehículos (fuente y destino), se usa la técnica multi-hop (Múltiples saltos) para enviar los paquetes de datos de vehículo a vehículo hasta alcanzar el destino correspondiente. (Giraldo, 2013)

Se define entonces a las Redes VANETs como una clase de red inalámbrica derivada de las Redes *MANET (Mobile Ad-hoc Networks*), que han surgido gracias a los avances tanto en las tecnologías inalámbricas e investigaciones en la industria automotriz para desarrollar Redes que permiten la comunicación entre vehículos a diferentes

velocidades. En las redes vehiculares, cada vehículo es equipado con la tecnología necesaria para permitir capturar información de sí mismo como de su entorno, esta información no solo debe ser procesada para la toma de decisiones del mismo vehículo sino que también para ser transmitida a los demás vehículos adyacentes o dentro de la topología. (Giraldo, 2013)

3.2.2 Características Redes VANETS

Debido a que en las Redes VANETs los vehículos pueden establecer una comunicación entre ellos y con algún tipo de infraestructura. Las Redes vehiculares tienen las siguientes características según (Batista, 2012) y (Giraldo, 2013):

- **Autonomía:** cada terminal es un nodo autónomo con capacidad para procesar y enrutar la información proveniente de otros nodos de la misma red.
- **Control distribuido de Red:** el control se hace en cada nodo ya que no se tiene infraestructura que lo realice.
- **Enrutamiento**: es necesario que cada nodo por separado, y todos en conjunto, provean un mecanismo dinámico de enrutamiento. Los protocolos clásicos de enrutamiento no son aplicables a este tipo de redes ya que no están preparados para las variaciones de topología que presentan las VANET. Actualmente, se están desarrollando algoritmos de enrutamiento para enfrentar este problema.
- **Topología de Red variable**: en las redes vehiculares los nodos o vehículos se pueden mover de forma arbitraria, aunque a veces sigan algunos patrones de movilidad. Debido a esto, las Redes se pueden subdividir y por consiguiente, pueden experimentar la pérdida de paquetes. Para esto se deben desarrollar mecanismos que detecten estas circunstancias y que minimicen de esta forma sus efectos.

En una VANET la topología de la red y la conectividad son diferentes respecto a los clásicos modelos de redes ad-hoc. El hecho de que los vehículos se están moviendo y cambiando de posición, hace que la topología de la red cambie frecuentemente con la conexión y desconexión de los enlaces entre los nodos.

- **Energía Ilimitada**: los inconvenientes de alimentación de los dispositivos móviles, no constituyen una limitación importante para las Redes vehiculares, ya que el propio nodo (vehículo), puede proporcionar energía permanente a los dispositivos informáticos y de comunicación.
- **Mayor Capacidad Computacional:** las Redes vehiculares requieren a menudo brindar mayores capacidades de detección, comunicación y cómputo, por lo que los vehículos y las estaciones deben de contar con muy buenos equipos computacionales.
- **Movilidad Predecible:** Por lo general los vehículos tienden a tener movimientos de fácil predicción, al estar limitados por el diseño de las carreteras. Con la tecnología GPS, es posible conocer la posición exacta del vehículo, con esta información y sabiendo además la trayectoria y velocidad de desplazamiento del mismo, se puede predecir las posiciones de sus nodos.

  Una ventaja en este tipo de redes es que la movilidad de los vehículos está limita por factores como calles, semáforos, límites de velocidad, entre otras. Así mismo, la existencia de sistemas de transporte: buses, trenes, sistemas automáticos, etc., nos permite tener una mayor predictibilidad de la red con respecto a las MANETs. Otro punto importante a considerar, es que el rango de cobertura de los radios usados, usualmente va desde los 100 hasta los 300 metros, lo que ayuda en el intercambio eficiente de información entre vehículos.
- **Escala Potencialmente Grande:** Las Redes vehiculares se extienden sobre toda la red vial, aumentando de tal forma el tamaño de la red, esto implica la

participación de un elevado número de nodos, que requieren niveles de potencia elevados para ampliar su rango de cobertura y mantener las comunicaciones.

- **Alta Movilidad:** las Redes vehiculares operan sobre un entorno altamente dinámico. Los vehículos en las carreteras viajan a velocidades muy altas (100Km/h en autopistas y 60Km/h en la ciudad), lo cual conlleva a predecir que el periodo de comunicación inter-vehicular pueda ser muy corto.

  La topología de la red tiende a cambiar de forma aleatoria y rápida en todo momento, dificultando el establecimiento de la conectividad de la red, la cual debe mantenerse estable para que los servicios de comunicación puedan operar sin inconvenientes. En este caso el protocolo de enrutamiento debe modificarse o ajustarse.

- **Ancho de banda limitado:** el ancho de banda en sistemas inalámbricos, que carecen de infraestructura física y más con dicha movilidad es mucho más reducido que el ancho de banda de redes que están preestablecidas.

  Fluctuación de los enlaces: La calidad de la información se ve afectada a medida que los saltos entre los nodos de las Redes Ad Hoc se va incrementando debido a la adición de errores de bit entre cada salto. La información tarda mucho en entregar los paquetes al destinó requerido.

Con todas estas características VANET es una tecnología que ha ido emergiendo y se ha convertido en un soporte importante para el desarrollo de los Sistemas Inteligentes de Transporte (ITS).

3.2.3 Frecuencias de operación VANET

Las redes vehiculares ad-hoc, al igual que las redes MANET, por lo general trabajan en una determinada banda de frecuencia que se localiza en las bandas no licenciadas de 2.4 GHz, 5 GHz y 914 MHz. Un gran número de investigadores enfocan sus estudios

sobre el desarrollo de esta tecnología trabajando sobre la banda de 5.9 GHz. (Luis Alberto Caldas Calle, 2013)

En estas bandas se manejan velocidades aceptables para transmisión de información entre vehículos y dentro del perímetro establecido por el alcance y cobertura de la red inalámbrica. (Luis Alberto Caldas Calle, 2013)

3.2.4 Arquitectura redes vehiculares VANET

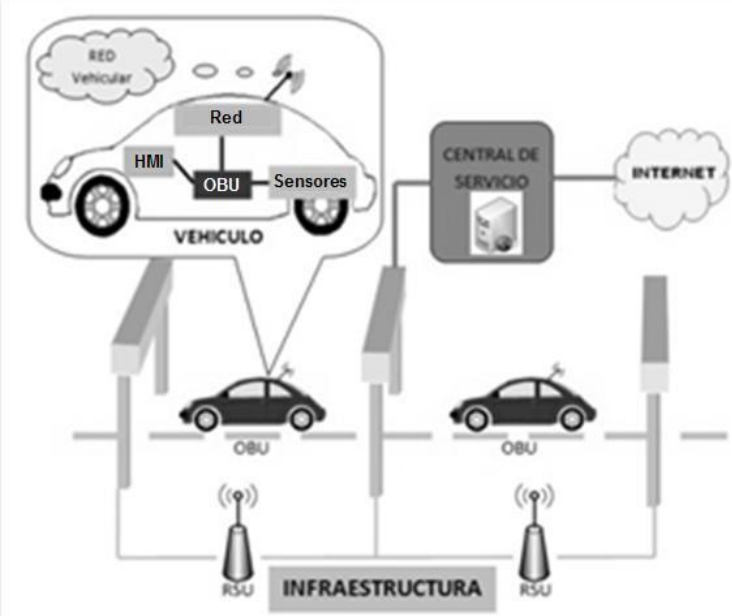


Figura 43. Sistema ITS en Carretera

Fuente: (Antoni Gabriel Caicedo Bastidas, 2011)

3.2.5 Principales elementos VANET

(Antoni Gabriel Caicedo Bastidas, 2011), explica los elementos principales de una red VANET:

1) ***Vehículo**:* Este conforma la parte principal dentro de la arquitectura **ITS**, ya que toda la funcionalidad desplegada se centra en la mejora de su circulación y hacen uso de un conjunto de servicios ITS que están destinados a mejorar su seguridad, hacer más eficiente su circulación y ofrecer un confort mejorado.

Dentro de este elemento se encuentran todo un conjunto de dispositivos que ayudan a monitorear el vehículo y el entorno en el que se mueve, entre ellos están: **Unidad abordo (OBU, On Board Unit)** [5], **Interfaz de usuario (HMI, Human Machine Interface),** módulo de comunicaciones y sensores.

En dichos sistemas de abordo, es posible incluir el software necesario para ofrecer una arquitectura escalable, así como para ofrecer servicios que requieran de las comunicaciones con el exterior. Dicho computador está ligado a un componente hardware/ software de interfaz con el usuario, de forma que el usuario pueda interactuar debidamente con las aplicaciones de la OBU. Las comunicaciones en ambientes vehiculares y la viabilidad de la transmisión de servicios como los de voz y video IP, son elementos fundamentales.

2) ***Infraestructura**:* está formada tanto por el hardware distribuido a lo largo de las carreteras, como por el hardware centralizado en los nodos de comunicación. El componente fundamental de este elemento es la unidad a un lado de la carretera **(RSU, Road Side Unit),** como su nombre lo indica, se sitúa a un lado de la carretera, y principalmente, está formado por sensores de diversa índole, tales como: *detectores de paso de vehículos, de temperatura, sistemas de reconocimiento de imágenes, radares de velocidad,* etc. No obstante, el hardware instalado en la carretera que más está ganando interés en los últimos años es el relacionado con las comunicaciones.

3) **Central de Servicios:** la finalidad de la central de servicios es disponer de las aplicaciones finales. Los servicios que se encuentran en este nivel pueden estar orientados a la gestión centralizada, como es el caso de los sistemas de

monitorización y seguimiento, o destinados a la provisión de funcionalidades a los vehículos, como serán los *servicios de información de tráfico o de gestión de reservas de parqueaderos, etc*.

3.2.6 Descripción general de la estructura VANET

En (Luis Alberto Caldas Calle, 2013), se explica que las redes vehiculares ad-hoc, en su forma general, constan de dos tipos de nodos: los nodos estáticos y los nodos móviles. Los nodos estáticos mejor conocidos como **RSU (Road Side Unit**), son elementos fijos, ubicados a lo largo de las carreteras, cuya función es enviar, recibir y retransmitir paquetes para incrementar el rango de cobertura de la red. En cuanto a los nodos móviles, son vehículos equipados con un dispositivo electrónico conocido como **OBU (On Board Unit)** que le permite establecer una comunicación con otros vehículos o con las **RSU**.

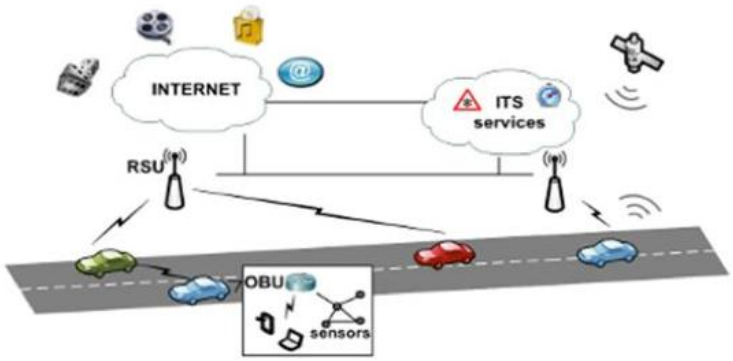


Figura 44. Representación General de los elementos de una VANET
Fuente: (Luis Alberto Caldas Calle, 2013)

Las Redes Ad-Hoc se pueden clasificar en dos diferentes arquitecturas que se definen según la estructura que forman al construirse la red, *la arquitectura plana y la arquitectura jerárquica.* (Giraldo, 2013)

La Arquitectura VANET de referencia, propuesta por el Car-to-Car Communication Consortium (C2C-CC) que se aprecia en la Figura 45*;* distingue tres dominios de comunicación en las redes vehiculares: *Dominio en Vehículo, Dominio Ad-Hoc y Dominio Infraestructura* (Giraldo, 2013).

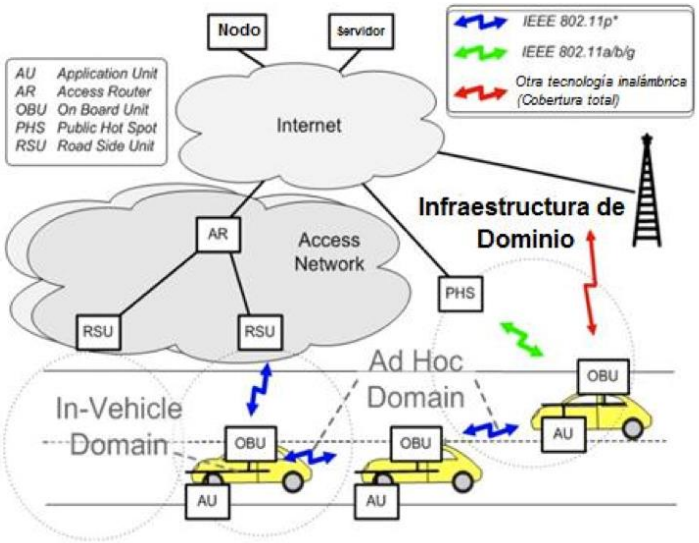


Figura 45. Arquitectura de referencia para redes vehiculares C2C-CC

Fuente: (Giraldo, 2013)

El **Dominio en Vehículo**, se refiere a una red local dentro de cada vehículo, compuesta evidentemente por dos tipos de unidades como lo podemos observar en la (Figura 45): La **On-Board Unit (OBU):** Una OBU es un dispositivo en el vehículo, que tiene capacidades de comunicación inalámbrica o cableada. (Giraldo, 2013)

La **AU**: Es un dispositivo que ejecuta una o múltiples aplicaciones; mientras hace uso de las capacidades de comunicación de la OBU. Las AU pueden ser los computadores portátiles, PDAs, smartphones, que se conectan de forma dinámica a una OBU. (Giraldo, 2013)

El **Dominio Ad-Hoc,** se refiere a una comunicación vehículo a vehículo (V2V) sin apoyo de la Red de infraestructura (Figura 44). Aquí la Red se compone por los vehículos equipados con **OBUs** y las **RSUs** que se fijan a lo largo de la carretera, para mejorar la seguridad vial; mediante la ejecución de aplicaciones especiales, o el envío, recepción y retransmisión de datos a las unidades vehiculares. Las OBUs de diferentes vehículos forman la Red Ad-Hoc móvil (MANET), donde cada OBU integra características inalámbricas de comunicación; homogéneas o heterogéneas, que definen el rango de cobertura o limitan la propagación. (Giraldo, 2013)

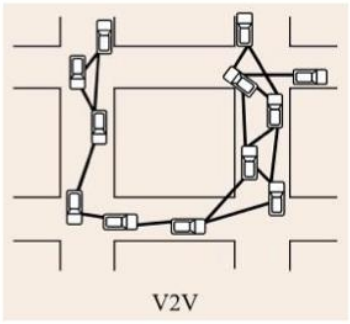
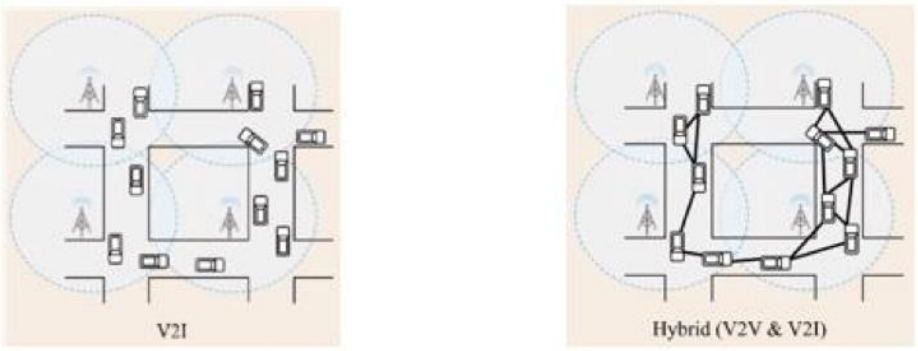


Figura 46. Comunicación vehículo a vehículo (V2V)

Fuente: (Giraldo, 2013)

El **Dominio Infraestructura**, como su nombre lo indica; se refiere a la comunicación vehicular, con soporte de la red de infraestructura. El acceso a ella, puede ser por intermedio de las RSUs y Hotspots públicos, comerciales o privados; o también aprovechando las capacidades de comunicación de las redes celulares y tecnologías radio (GSM, GPRS, UMTS, WIMAX) integradas como parte del equipamiento OBU de las unidades vehiculares, en caso de que los terminales RSUs y Hotspots sean insuficientes. (Giraldo, 2013)



(a) (b)

(b)

Figura 47. Comunicación vehicular (a) Vehículo-infraestructura, (b) Híbrida

Fuente: (Giraldo, 2013)

Las Redes Ad-Hoc utilizan tecnologías inalámbricas diferentes para la comunicación entre sus dominios, como es la **WLAN** basada en el estándar **IEEE 802.11**, la de comunicación dedicada a corto alcance (**DSRC**) y la tecnología **GPRS2/ UMTS3**. En la (Figura 47) se aprecia la comunicación vehicular que se presenta en el dominio de la Infraestructura, donde se destaca un modelo Híbrido y se observa la comunicación que existe vehículo a vehículo (V2V), vehículo a infraestructura (V2I) y viceversa. (Giraldo, 2013)

3.2.7 Información del sistema- problemas frecuentes VANET

Según (Batista, 2012) y (Toutouh, 2013) a continuación se explican los problemas frecuentes de las redes VANET:

- La caracterización de una VANET pasa por la definición de un modelo para la comunicación inalámbrica, uno para la distribución de los vehículos y otro para la estructura de la red.
- Se considera un escenario típico para un recorrido de transporte público. La red se representa como una sección de ruta, con dos puntos, origen y destino,

conocidos de antemano, donde cada vehículo entra y sale a la red por el punto respectivo, y viaja a una velocidad promedio. Se asume que cada RSU y OBU de la red utilizan la misma tecnología de comunicación, y tienen un radio de cobertura R. La existencia de un enlace V2I, o V2V dependerá de la función de conexión de acuerdo al modelo de canal inalámbrico que se utilice. Se analizará para el modelo de comunicación de disco unitario y para el modelo con desvanecimiento log-normal. Además, no se presentan restricciones de energía, y todas las transmisiones se asumen omnidireccionales.

- El estándar IEEE 802.11p, basado en comunicaciones directas de corto alcance (**DSRC**), se ha definido expresamente para el acceso al medio inalámbrico en entornos vehiculares (**WAVE**).
- La limitada cobertura del estándar IEEE 802.11p y la alta movilidad de los nodos provoca que los enlaces que se crean durante la comunicación tengan un tiempo de vida muy limitado, lo que complica de forma crítica el correcto intercambio de paquetes (frecuentes cambios de topología y fragmentación de la red). Así, el encaminamiento (routing) eficiente de paquetes en redes vehiculares es una tarea altamente compleja.
- Las VANETs requieren de un servicio de difusión (broadcasting) de mensajes para el descubrimiento de nodos cercanos y el envío de información. Sin embargo, en situaciones de tráfico denso (número elevado de conexiones), aparece el problema de **tormenta por difusión**, congestionándose la red.
- Es importante disponer de una plataforma física para el despliegue de VANETs, es decir, de una infraestructura compuesta por nodos fijos (estaciones base) empleados para comunicar nodos móviles con redes estáticas (Internet) y con otros nodos móviles que estén fuera del alcance directo.

- La alta volatilidad y el gran dinamismo de las redes vehiculares limita la aplicación directa de protocolos de encaminamiento y difusión ya empleados en otras redes móviles ad-hoc (MANETs) en las comunicaciones V2V, apareciendo diversas líneas de trabajo para el diseño de protocolos específicos.

3.2.8 Funcionamiento

Las Redes VANETs empiezan a ejecutar o a realizar su trabajo desde sus nodos móviles, que son los vehículos que conforman la Red, estos buscan establecer una comunicación entre sí, una vez se instaura un intercambio de información entre ambos nodos se empieza a efectuar o desarrollar una de las características que alberga estas redes, como es la autonomía, donde cada uno de sus nodos tiene la capacidad de recibir, procesar, transmitir y enrutar información, cada nodo realiza el control de la información, la encamina y establece una comunicación entre los demás nodos de la red, permitiendo así enrutar los paquetes. (Giraldo, 2013)

Los nodos pueden desplazarse arbitrariamente entrando y saliendo de la red cuando lo considere necesario, esto se presenta debido a las altas velocidades de movilidad que los vehículos desarrollan, también por la capacidad variable que presentan los enlaces y por la cantidad de enlaces inalámbricos que debe cruzar en ciertos recorridos para poder llegar así a su destino. (Giraldo, 2013)

3.2.9 Conexión de las redes vehiculares a internet

La conexión a Internet de los vehículos permitiría que sus ocupantes pudieran acceder a multitud de servicios de información y utilizar cualquiera de los servicios comunes de las redes IP como la navegación web, correo electrónico, etc. (Tello, 2012)

La conexión de los vehículos a Internet se puede realizar a través de diferentes tecnologías de acceso. Por un lado, se pueden conectar las VANETs a la infraestructura a través de equipos situados al borde de las carreteras, denominados **Road Side Units (RSUs),** que actúan como puertas de enlace y que pueden proporcionar conexión a Internet porque están conectados a la infraestructura de red de algún operador. En este caso, las comunicaciones se llevan a cabo utilizando tecnologías inalámbricas de corto alcance o Dedicated Short-Range Communications (**DSRC**). **DSRC** engloba un conjunto de tecnologías de comunicaciones de corto alcance entre las que destacan las tecnologías **WiFi IEEE 802.11**, y especialmente **IEEE 802.11p**, que es una adaptación del estándar IEEE 802.11 para mejorar las prestaciones de las comunicaciones en escenarios de redes vehiculares. (Tello, 2012)

Por otro lado, se puede proporcionar a los vehículos conexión a Internet mediante tecnologías de comunicaciones móviles celulares **(GPRS, UMTS, LTE).** Se plantea el uso de redes celulares no solo para comunicaciones V2I, sino también para comunicaciones V2V aprovechando que las redes ya se encuentran desplegadas y que los operadores están continuamente mejorándolas. (Tello, 2012)

Por ello, el escenario que resulta más interesante, y cuyo despliegue parece más probable, es aquel que busca una solución hibrida donde los vehículos se encuentran equipados con múltiples tecnologías de comunicaciones y utilizan la más adecuada para cada situación. Por ejemplo, los vehículos podrían estar equipados con una interfaz 3G/LTE y una interfaz IEEE 802.11 de manera que la VANET fuera una red de acceso non-3GPP integrada en la arquitectura 4G. Este modelo sigue la tendencia que los operadores están impulsando que se basa en la utilización de redes de acceso heterogéneas para minimizar costes y proporcionar mejores prestaciones a los usuarios. (Tello, 2012)

Según (Tello, 2012) la conexión de los vehículos a Internet por medio de RSUs, presenta una serie de requisitos que hay que resolver:

- Despliegue de múltiples RSUs que actúen como puertas de enlace hacia Internet.
- Decidir si los vehículos se pueden conectar a las RSUs por medio de una comunicación multisalto a través de diferentes nodos de la VANET o, por el contrario, únicamente se permite la comunicación directa entre los vehículos y las RSUs (a un salto).
- Protocolo que gestione la conexión de los vehículos a las puertas de enlace hacia Internet o RSUs.
- Es necesario un protocolo de encaminamiento para establecer las rutas entre los nodos que forman la VANET y encaminar los paquetes entre los vehículos y las RSUs conectadas a Internet.
- Las VANETs tienen ciertas características especiales como la inestabilidad de los enlaces entre nodos provocada por la alta movilidad, y la variabilidad de la densidad de nodos en la red, que hacen que el correcto desempeño del protocolo de encaminamiento sea crítico para el buen funcionamiento de las comunicaciones.
- Debido a su movimiento, los vehículos cambian su punto de acceso a Internet continuamente conectándose a diferentes RSUs. Por ello, es necesario un protocolo que gestione la movilidad y que mantenga las comunicaciones de los vehículos activas a pesar del handover entre puntos de acceso.
- Centrándose en la gestión de la movilidad, esta se puede llevar a cabo en diferentes capas de la torre de protocolos, pero posiblemente la **gestión de la**

movilidad a nivel IP sea lo más conveniente, ya que es la capa común de la pila de protocolos.

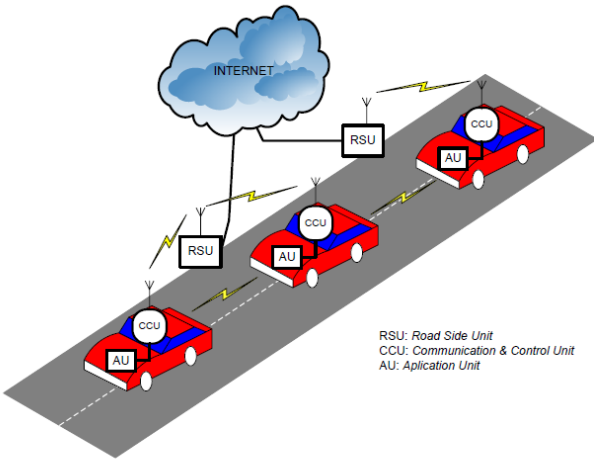


Figura 48. La arquitectura del sistema de transporte inteligente definida por el ETSI
Fuente: (Víctor Sandonís Consuegra, 2014)

Se describe la arquitectura del sistema de transporte inteligente que ha sido estandarizado por el ETSI (European Telecommunications Standards Institute) y el protocolo de GeoNetworking que se utiliza para las comunicaciones en la VANET. (Víctor Sandonís Consuegra, 2014)

3.2.10 Protocolos en redes vehiculares VANET

El IEEE 1609 Working Group ha estado trabajando en la familia de **protocolos IEEE 1609** para **Wireless Access in Vehicular Environments (WAVE)**. Este conjunto de estándares define la arquitectura, las interfaces y los protocolos para comunicaciones inalámbricas entre vehículos (V2V), y entre vehículos y la infraestructura (V2I). (Víctor Sandonís Consuegra, 2014)

Siguiendo un modelo divido en capas, los niveles físico y de enlace se corresponden con el estándar IEEE 802.11p [39] y el estándar IEEE 1609.4 [99], que se centra en la coordinación entre los diferentes canales de servicio (SCH) y el canal de control (CCH), y que utiliza técnicas de acceso al medio del estándar 802.11e Enhanced Distributed Channel Access (EDCA) [100] que permiten establecer prioridades de acceso al medio para diferentes tipos de tráfico. El nivel de red se corresponde con el estándar **IEEE 1609.3.** (Víctor Sandonís Consuegra, 2014)

3.2.11 Principales protocolos de enrutamiento en redes vehiculares VANETS

Según (Luis Alberto Caldas Calle, 2013) y (Domínguez, 2010), los protocolos que se utilizan para controlar el encaminamiento de los paquetes a intercambiar dentro de una red vehicular ad-hoc mantienen ciertas características propias de los protocolos desarrollados para MANET. La diferencia se da en el hecho de que deben soportar una topología escalable y variable. Entre los protocolos que funcionan en las redes MANET y que se consideran apropiados para ser utilizados para la simulación con VANETs destacan los protocolos **DSDV, AODV y TORA**.

3.2.11.1Arquitectura del sistema de transporte inteligente

Uno de los aspectos críticos para que los vehículos puedan conectarse a Internet de forma satisfactoria es que el protocolo de encaminamiento que se utiliza en la VANET ofrezca unas prestaciones adecuadas que permitan que las comunicaciones funcionen correctamente a pesar de la inestabilidad de los enlaces entre nodos, característica de las redes vehiculares. El estudio de prestaciones basado en simulación que se ha llevado a cabo ha revelado el comportamiento de los mecanismos del protocolo, resaltando sus limitaciones y puntos débiles. (Víctor Sandonís Consuegra, 2014)

3.2.11.2 Protocolo de geonetworking (GN)

Protocolo diseñado para el encaminamiento de los paquetes en la VANET tomando los requisitos de seguridad vial como punto principal y dejando en un segundo plano los aspectos relacionados con la conectividad a Internet. (Víctor Sandonís Consuegra, 2014)

3.2.11.3 Proxy mobile IPV6 (PMIPV6)

Adaptan PMIPv6 a la arquitectura multisalto del ITS. La solución permite a los vehículos mantener sus comunicaciones activas a pesar de los cambios de punto de conexión a Internet, sin que tengan que verse involucrados en los procedimientos de gestión de la movilidad. (Víctor Sandonís Consuegra, 2014)

3.2.11.4 Estándar IEEE 802.11P - WAVE

Es la propuesta del IEEE para un sistema estándar de comunicación vehicular. WAVE es una pila de protocolos que tiene soporte para tráfico TCP/IP, así como protocolos de transporte, red y de aplicación, ver Figura 49. (Antoni Gabriel Caicedo Bastidas, 2011)

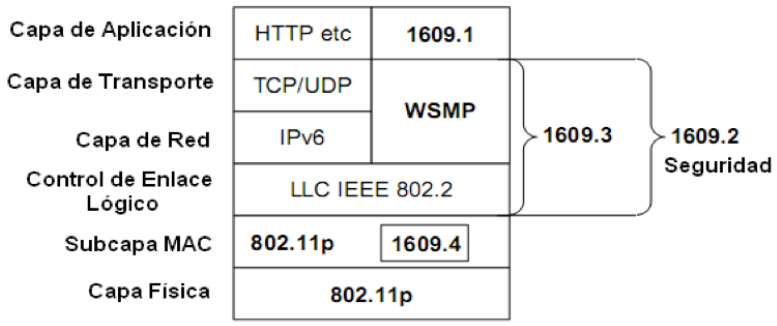


Figura 49. Visión General de la Pila de Protocolos WAVE

Fuente: (Antoni Gabriel Caicedo Bastidas, 2011)

Para hacer frente al dinamismo de los ambientes vehiculares el grupo de IEEE 802.11 desarrolló el estándar **IEEE 802.11p**, referenciado también como **WAVE (Wireless**

Access in Vehicular Environment), y cuya finalidad es asegurar la operatividad de la comunicación V2V y V2I que requiere un intercambio de datos de corta duración debido a la velocidad de los nodos. IEEE 802.11p tiene asignado el **espectro DSRC (Dedicate Short Range Communication)** con licencia en la banda de 5.9 GHz para Estados Unidos (y 5.8 GHz para Japón y Europa), ofreciendo transferencia de datos entre 6 y 27 Mbps a distancias medias de hasta 1km y a altas movilidades (velocidades de 200 km/h). (Batista, 2012)

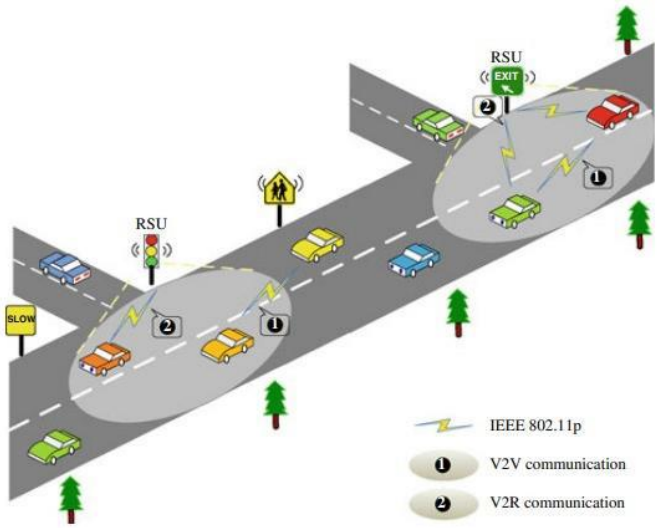


Figura 50. Arquitectura de una VANET híbrida.
Fuente: (Batista, 2012)

WAVE adopta de forma específica la denominación IEEE 802.11p, es una evolución del estándar IEEE 802.11a con modificaciones a nivel físico y MAC para mejorar su comportamiento en el entorno vehicular. Al igual que IEEE 802.11a, WAVE utiliza OFDM, pero con tasas de transmisión de 3, 4.5, 6, 9, 12, 18, 24, y 27 Mbps en canales de 10 MHz. Utiliza 52 sub-portadoras moduladas utilizando BPSK, QPSK, 16-QAM o 64-QAM así como codificaciones de ratios 1/2, 2/3, o 3/4. Además, IEEE 802.11p hereda los procedimientos de diferenciación de servicios que ya contemplaba la

extensión 802.11e mediante la creación de una serie de interfaces que permiten administrar el servicio de los paquetes según la prioridad que tengan asignada. (Giraldo, 2013) y (Domínguez, 2010)

Según (Giraldo, 2013) y (Domínguez, 2010), a continuación se describe la arquitectura WAVE:

WAVE (Wireless Access in Vehicular Environments) constituye la arquitectura de protocolos que administra las capas de nivel de Red, enlace, acceso al medio y física para las comunicaciones en VANETs, (Tomás Gabarrón, Egea López, & García Haro). En la (Figura 51) se puede apreciar la arquitectura de protocolos WAVE.

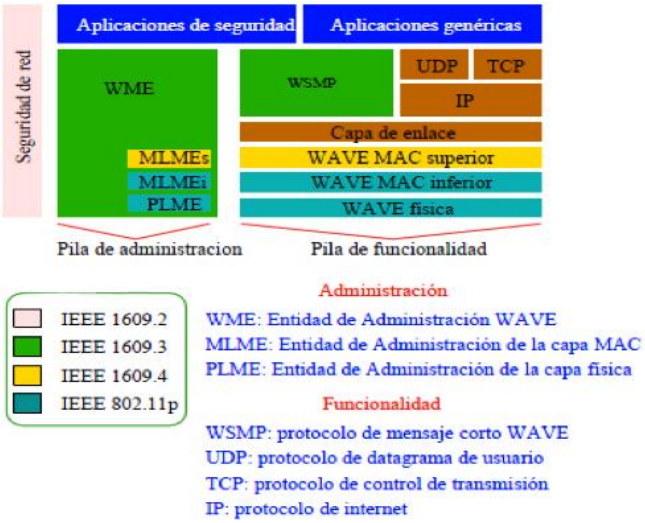


Figura 49. Arquitectura de protocolos WAVE (Wireless Access in Vehicular Enviroments)

Fuente: (Antoni Gabriel Caicedo Bastidas, 2011)

3.2.11.5 DSRC (Dedicated Short Range Communications).

La historia de la arquitectura WAVE se remonta a 1999 cuando la *FCC (Federal Communications Commission)* estadounidense estableció un espectro de 75 MHz en la banda de los 5.9 GHz (banda de los ITS, Sistemas Inteligentes de Transporte) para

albergar de manera exclusiva las tecnologías emergentes de radiocomunicaciones que tendrían lugar en las Redes vehiculares de nueva generación. (Giraldo, 2013)

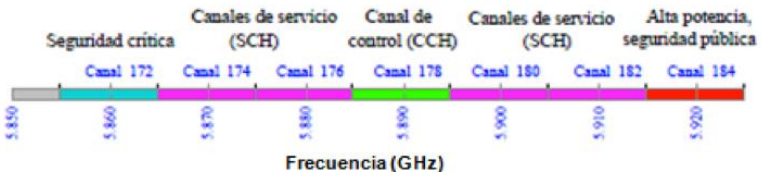


Figura 52. Estructura del espectro en la banda de los SIT (Sistemas Inteligentes de Transporte)

Fuente: (Antoni Gabriel Caicedo Bastidas, 2011)

La (Figura 52) muestra el espectro que adopta el DSRC en esta banda, y se estructura según siete canales de 10 MHz cada uno. (Giraldo, 2013)

3.2.12 Aplicaciones VANETS

Uno de los principales objetivos de los Sistemas Inteligentes de Transportes (ITS) es poder brindar un mejor escenario de conocimiento de las carreteras a los conductores, para de cierta forma poder reducir el número de accidentes y a su vez la conducción se pueda realizar de una manera más cómoda y fluida. (Giraldo, 2013)

Para las redes que permiten la comunicación de vehículo a vehículo como lo son las redes VANETs, las aplicaciones pueden ir desde un simple intercambio de información entre sus nodos, hasta el poder tener acceso a contenidos multimedia e internet, los beneficios de estas redes vehiculares se pueden ver más en detalle en las siguientes aplicaciones (Giraldo, 2013), (Serrano, 2012):

- **Aplicaciones de seguridad vial.**

Las aplicaciones orientadas a la seguridad vial tienen como finalidad ayudar a mejorar la seguridad de los conductores. Las comunicaciones vehiculares permiten que los vehículos puedan intercambiar entre sí información sobre su posición, velocidad y dirección, de manera que esta se pueda utilizar para evitar colisiones por frenazos bruscos o atascos repentinos informando con antelación al conductor cuando se detecta que existe la posibilidad de colisionar con otro vehículo. Si en el peor de los casos se detecta que la colisión entre vehículos es inevitable, se podrían tomar las medidas oportunas para minimizar los daños de los ocupantes de los vehículos mediante mecanismos de frenado automático o la activación de los airbags antes del impacto.

Otro ejemplo de caso de uso es la utilización de las comunicaciones vehiculares para difundir mensajes de alerta en la VANET para informar a los conductores sobre puntos conflictivos o zonas peligrosas en la carretera con suficiente antelación. Por ejemplo, si un vehículo dispone de un sensor que detecta que la carretera esta resbaladiza por una mancha de aceite en una curva, se puede generar un mensaje de alerta que se hace llegar al resto de conductores. De esta forma, si un motorista recibe el mensaje de alerta, puede estar atento y evitar una posible caída.

- **Aplicaciones orientadas a la eficiencia del tráfico.**

Dentro de este grupo se encuentran todas las aplicaciones orientadas a mejorar la fluidez del tráfico que se traduce en un menor consumo de tiempo y combustible para los conductores y un mejor aprovechamiento de las infraestructuras viales. Además, de manera indirecta se reduce el impacto medioambiental de la contaminación producida por los vehículos.

Las VANETs permiten a los vehículos difundir mensajes con información sobre su posición geográfica que pueden ser recopilados para calcular el estado del tráfico en diferentes zonas geográficas. De esta manera, se puede desarrollar un sistema que se encargue de recopilar esta información en un centro de control de tráfico y calcule el estado del tráfico en las carreteras en tiempo real (por ejemplo, obteniendo parámetros de densidad, flujo de vehículos y velocidades medias). Del mismo modo, este sistema puede difundir mensajes en la VANET que señalen a los conductores las mejores rutas a seguir para evitar zonas congestionadas en función de las condiciones de tráfico actuales.

Otro ejemplo de caso de uso es aquel en el que se facilita a los vehículos la incorporación a una autovía o autopista. Para ello, teniendo en cuenta las condiciones de circulación de la vía, se informa a los conductores sobre la velocidad deben llevar para realizar una incorporación adecuada sin interrumpir la fluidez del tráfico.

Siguiendo la misma idea, en una intersección regulada por semáforos, se puede difundir mensajes con información del estado y temporización de los mismos. Así, los vehículos que se aproximan a la intersección pueden utilizar esta información para indicar al conductor la velocidad adecuada que debe llevar para evitar parar en la intersección innecesariamente, ahorrando combustible y reduciendo la contaminación.

- **Aplicaciones de entretenimiento y servicios de información**

Un caso de uso sería un servicio de notificaciones de puntos de interés mediante la difusión de mensajes en la VANET. Por ejemplo, una gasolinera difunde información en la VANET sobre sus precios, que puede ser de interés para aquellos conductores que circulan en su cercanía. Del mismo modo, se puede proporcionar información a los

conductores de la ubicación de los parkings más cercanos a su posición, su estado de ocupación, precios, etc.

3.2.13 Aplicación específica VANET- Arquitectura VANET para monitoreo de calidad de aire

El sistema propuesto por (Giuseppe Lo Re, 2014) está compuesto por algunos nodos sensores vehiculares, un servidor de monitoreo y algunos puntos de acceso instalados en las carreteras. Los componentes principales son:

• Nodos en el vehículo, cada uno provisto de un microcontrolador, dispositivos de comunicación y sensores.

• Gateways, reciben datos de cada nodo y los envían al servidor central.

• Servidor central, almacena los datos recopilados, asegurando la integridad, seguridad y disponibilidad.

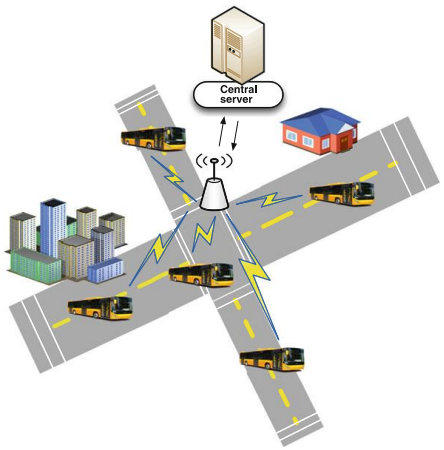


Figura 53. Arquitectura VANET para monitoreo de la calidad de aire

Fuente: (Giuseppe Lo Re, 2014)

3.2.13.1 Funcionamiento

Cada nodo vehicular consta de una unidad central y una placa sensora (sensor board). Periódicamente, la unidad central recoge la concentración detectada de contaminación del aire de la tarjeta sensora y almacena los datos junto con el tiempo y la ubicación actual dados por el módulo de Sistema de Posicionamiento Global (GPS). Este dispositivo es tan responsable de la agregación, sincronización y transmisión de datos detectados al servidor central para su almacenamiento y posterior procesamiento. La comunicación se otorga a través de una arquitectura centralizada Vehículo a Infraestructura (V2I). Vehículo a Infraestructura se refiere a la conexión entre vehículos y puntos de acceso fijos, también llamados Unidades de Lado de Carretera (RSU), que requieren la colocación de tales dispositivos de comunicación en estructuras externas, o en lugares convenientes, tales como intersecciones, semáforos o edificios. Una RSU actúa como punto intermedio para el intercambio de información entre vehículos, por lo que su principal tarea es ampliar la red enviando datos procedentes de vehículos, a servidores centralizados o, eventualmente, a otros vehículos próximos. (Giuseppe Lo Re, 2014)

La aplicación diseñada es tolerante al retardo y basada en el tiempo, por lo que no tiene ninguna obligación restrictiva de enviar datos en tiempo real al portal. En su lugar, cada vehículo obedece a una política de diseminación de tiendas y difusión. Recoge los datos de los sensores, periódicamente a intervalos regulares, y los procesa localmente antes de enviarlos al servidor central usando puntos de acceso inalámbricos encontrados de manera oportunista de una manera tolerante al retardo. En particular, cada nodo de la red mantiene los datos en su propia memoria esperando por un punto de acceso remoto dentro del rango para transferir los datos detectados a un servidor central. De esta forma

es posible reducir el número de conexiones entre RSUs y vehículos, manteniendo al mismo tiempo alta precisión y control de calidad. Aprovechando la conectividad ofrecida por el punto de acceso, el nodo carga los datos detectados en el servidor, donde la información sensorial puede estructurarse mediante una ontología para su posterior análisis, uso compartido o reutilización. (Giuseppe Lo Re, 2014)

3.2.13.2 Implementación

En esta sección se analiza los componentes de hardware necesarios para implementar el sistema descrito. Para realizar un nodo de red se elige un microcontrolador Arduino, conectado a un receptor GPS para información de posición global, un módulo inalámbrico para la comunicación por radio y una tarjeta de sensor de gas personalizada para medir la calidad del aire. (Giuseppe Lo Re, 2014)

Arduino es una plataforma de creación de prototipos de electrónica de código abierto, basada en hardware y software flexible y fácil de usar. Arduino se basa en una arquitectura modular, de hecho la idea es integrar fácilmente sólo los módulos necesarios en cada dispositivo. El entorno de desarrollo y las bibliotecas suministradas se pueden modificar fácilmente mediante el lenguaje C/ C ++. Entre las diferentes placas de Arduino, elegimos el microcontrolador Arduino Mega 2560 para nuestra implementación de prototipos. En particular, el Arduino Mega 2560 se basa en el microcontrolador Atmel ATmega2560 que ofrece 54 pines de E/ S digitales, 16 entradas analógicas, 4 puertos UART, un reloj de 16 Mhz, una conexión USB y un cabezal ICSP. El gran número de clavijas de E/ S facilita la inclusión de sensores de gas y otros componentes de comunicación como el modulo Xbee Pro para la transmisión de datos. (Giuseppe Lo Re, 2014)

El núcleo del sistema de monitoreo es la placa sensora de gas provista de varios sensores semiconductores. Estos sensores explotan el cambio de la conductividad causada por la absorción de contaminantes gaseosos sobre una superficie semiconductora. Sus entradas comprenden un soporte en diversos materiales tales como aluminio, silicio y cerámica, una resistencia de calentamiento y una capa de detección que está compuesta de un material de óxido metálico tal como dióxido de estaño (SnO2) o óxido de cinc (ZnO). A temperatura de trabajo, se establece un conjunto de reacciones electroquímicas entre el oxígeno atmosférico y los gránulos de óxido. Estas reacciones modulan y regulan el flujo electrónico entre los granos del elemento sensor, cambiando su resistividad, y dando así información sobre una concentración precisa de gas. Estos dispositivos son particularmente sensibles a los cambios de temperatura, por lo tanto es necesario controlar el flujo de aire dirigido hacia la cabeza del sensor cuando está montado en un vehículo en movimiento. El comportamiento del sensor con respecto a los cambios de temperatura no es definible por una ecuación matemática, y la caída de temperatura del elemento de calentamiento induce un error en las medidas de concentración de gas. Este efecto es insignificante para concentraciones bajas de gases, pero se vuelve significativo para mayores niveles de contaminación. (Giuseppe Lo Re, 2014)

Con el fin de validar el diseño propuesto, en una fase preliminar, el VSN será desplegado en un solo vehículo perteneciente a la flota de autobuses de transporte público de Palermo y unos pocos puntos de acceso. Esta plataforma instalada en el bus supervisará los siguientes parámetros: Temperatura, Humedad relative, Dióxido de nitrógeno (NO2), Dióxido de carbono (CO2), Monóxido de carbono (CO), Ozono (O3). (Giuseppe Lo Re, 2014)

Para la recopilación de datos, algunos puntos de acceso basados en Xbee se instalarán en las calles, y se comunicarán con un servidor central que se puede implementar en una computadora de un solo tablero de bajo consumo, como el tablero Raspberry Pi. El Raspberry Pi, diseñado para ejecutar sistemas operativos basados en kernel Linux, está basado en un procesador ARM1176JZF-S de 700 MHz, e incluye 512 MB de RAM, dos puertos USB, salida de audio y video y usa una tarjeta Secure Digital como arranque y almacenamiento a largo plazo. En la placa Pi Lighttpd, una aplicación de servidor web ligero, permite al Pi servir páginas HTML dinámicas respaldadas por una base de datos SQLite, en la que la información recopilada está organizada de tal manera que asegura la integridad, seguridad y disponibilidad. (Giuseppe Lo Re, 2014)

3.2.13.3 Conclusión de la aplicación

La contaminación atmosférica urbana es una cuestión crucial para muchas zonas urbanas, por lo que es necesario vigilar y controlar la concentración de contaminantes de gas. Las redes de sensores vehiculares son un interesante desarrollo reciente en redes inalámbricas y móviles. Son extremadamente multifuncionales y pueden ser útiles para diferentes aplicaciones, como el monitoreo ambiental. Hemos propuesto una arquitectura VSN para el monitoreo de la calidad del aire urbano. La principal ventaja de nuestro enfoque es la economía y la simplicidad del sistema. Con sólo unos pocos vehículos pertenecientes a una flota de transporte público, se puede desplegar un sistema de monitoreo de grano fino capaz de cubrir todas las áreas de la ciudad. Además, proponemos el uso de la ontología como la herramienta más adecuada para permitir una cooperación máquina a máquina eficiente. (Giuseppe Lo Re, 2014)

3.3 Comparación tecnologías enfocadas en aplicaciones vehiculares

Gran parte de las investigaciones coinciden en que la conectividad en VANETs es influenciada principalmente por factores como: la densidad de vehículos, el rango de transmisión de los dispositivos de comunicación, las condiciones del ambiente (urbano o rural), la movilidad de los nodos, y la presencia de infraestructura en la red. En consecuencia la conectividad ha sido estudiada desde varios enfoques. (Batista, 2012)

A continuación se presenta un cuadro comparativo de las tecnologías que se pueden utilizar en el desarrollo de aplicaciones vehiculares, las cuales han sido referidas en el presente capítulo.

TABLA 5. CUADRO COMPARATIVO DE TECNOLOGÍAS PARA EL DESARROLLO DE APLICACIONES VEHICULARES.

COMPARACIÓN DE TECNOLOGÍAS PARA APLICACIONES EN ENTORNOS VEHICULARES			
ESPECIFICACIONES TÉCNICAS	**SENSOR CLOUD (Plataforma formada por WSN y Cloud Computing)**	**GPRS (Servicio de paquetes via radio)**	**VANET (Redes enfocadas a entornos vehiculares)**
TECNOLOGÍA O ESTÁNDAR	Estándares de WSN y Cloud computing: Aplicaciones y Servicios basados en servicios web.	Estándar GPRS. Utiliza TDM	Estándar IEEE 802.11p
PROTOCOLOS	Protocolos de enrutamiento WSN y TCP/IP	TCP/IP, X.25	Protocolos IEEE 1609- Wireless Access in Vehicular Environments (WAVE)
	IEEE 802.15.4- ZIGBEE	Capa de Aplicación. Protocolos específicos de cada aplicación.	Protocolo de GeoNetworking
	IEEE 802.11- WIFI	Protocolo túnel GPRS (GTP)	
	IEEE 802.15.3 - WPAN	Protocolo GPRS	
	Protocolos de Cloud Computing: TCP, IP, SMTP, HTTP		
VELOCIDAD DURANTE UNA SESION DE TRANSMISIÓN DE DATOS	Depende de la tecnología inalámbrica y estándar que se utilice. Si utiliza ZigBee la velocidad de transferencia es hasta 250Kbps.	52kbits/s o 171.2kbits/s	6 y 27 Mbps
FRECUENCIAS DE OPERACIÓN	Depende de la tecnología inalámbrica y estándar que se utilice, en el caso de ZigBee: 2,4 y 5GHz.	GPRS-2G-banda 2 (1900 MHz)	Bandas no licienciadas 2.4 GHz, 5 GHz y 914 MHz
ADMINISTRACIÓN DE ENERGÍA	Los nodos tienen energía de forma continua a través de la bateria del vehiculo. La red WSN tiene mecanismos de optimizacion de energía.	Los nodos tienen energía de forma continua a través de la bateria del vehiculo.	Los nodos tienen energía de forma continua a través de la bateria del vehiculo.
ALMACENAMIENTO	Nube- Ilimitado	Base de datos local	Local

TABLA 5. CUADRO COMPARATIVO DE TECNOLOGÍAS PARA EL DESARROLLO DE APLICACIONES VEHICULARES.

ESPECIFICACIONES TÉCNICAS	SENSOR CLOUD (Plataforma formada por WSN y Cloud Computing)	GPRS (Servicio de paquetes via radio)	VANET (Redes enfocadas a entornos vehiculares)
PROCESAMIENTO	Procesamiento en tiempo real en la nube	Local. Se procesa en el sistema.	Grandes capacidades de memoria y procesamiento local.
ENRUTAMIENTO	Se usan protocolos de enrutamiento de las redes de sensores inalámbricos según la estructura de la red o según la operación del protocolo.	El protocolo de túnel GPRS (GTP) garantiza la seguridad en la red troncal y simplifica el mecanismo de enrutamiento y la entrega de datos por la red GPRS.	Requiere mecanismos dinámicos de enrutamiento.
ACCESIBILIDAD	Accesibilidad común debido a protocolos estandarizados (TCP/IP) e interfaces.	Diferentes interfaces de hardware (e.g. RS232, USB, protocols propietarios) en diferentes máquinas.	Diferentes interfaces de hardware (e.g. RS232, USB, protocols propietarios) en diferentes máquinas.
UTILIZACION DE TIEMPO REAL	Tiempo y acceso en tiempo real de espacio libre a una gran cantidad de datos de sensor sin condiciones.	Acceso limitado de acuerdo a propiedades de hardware (e.g., puertos) ya que las máquinas físicas no pueden acceder y alojan un número ilimitado de dispositivos.	Acceso limitado de acuerdo a propiedades de hardware (e.g., puertos) ya que las máquinas físicas no pueden acceder y alojan un número ilimitado de dispositivos.
SEGURIDAD	Transmisión de datos inalámbricos por medio de un canal seguro SSL y envío de datos encriptados a la nube.	Con el fin de proteger contra errores los paquetes transmitidos tiene lugar la codificación del canal radio, mediante el método GEA (GPRS Encryption Algorithm, algoritmo de cifrado GPRS) con algoritmos secretos. El cifrado en GPRS abarca desde las funciones de cifrado del terminal móvil hasta las funciones de cifrado en el SGSN.	Mecanismos de seguridad a través del protocolo WAVE: IEEE 1609.2. Encriptar datos con una clave simétrica one-time.

TABLA 5. CUADRO COMPARATIVO DE TECNOLOGÍAS PARA EL DESARROLLO DE APLICACIONES VEHICULARES.

ESPECIFICACIONES TÉCNICAS	SENSOR CLOUD (Plataforma formada por WSN y Cloud Computing)	GPRS (Servicio de paquetes via radio)	VANET (Redes enfocadas a entornos vehiculares)
SINCRONIZACION GLOBAL	Alineación y sincronización de datos de sensores a gran escala debido a un tiempo global común posible.	Difícil alineación y proceso de sincronización debido a los diferentes mecanismos de sincronización de máquinas y dispositivos de sensores físicos a la deriva.	Difícil alineación y proceso de sincronización debido a los diferentes mecanismos de sincronización de máquinas y dispositivos de sensores físicos a la deriva.
PRESERVACIÓN DE DATOS	Reutilización de los datos de los sensores capturados como si se suministrara mediante un sensor en tiempo real. El acceso común como almacenamiento y protocolo se define (por lo tanto, intercambiable)	La captura y la preservación de los datos para volver a reproducirlos en un momento posterior debe desarrollarse para cada dispositivo físico. No hay almacenamiento y protocolo común y unificado.	La captura y la preservación de los datos para volver a reproducirlos en un momento posterior debe desarrollarse para cada dispositivo físico. No hay almacenamiento y protocolo común y unificado.
ESCALABILIDAD MÚLTIPLE	Acceso concurrente y fácil de una variedad de dispositivos sensor que funcionan bien a gran escala.	Acceso limitado y restringido, posibles cuellos de botella en el rendimiento y problemas de escalabilidad.	Acceso limitado y restringido, posibles cuellos de botella en el rendimiento y problemas de escalabilidad.
PODER DE CÓMPUTO	Recursos computacionales mejorados en la nube permiten la ejecución de métodos complejos	Recursos limitados según la máquina local	Recursos limitados según la máquina local
APLICACIONES	Salud Ubicua	RTI (Road Traffic Informatics)	Acceso a internet y descargas multimedia en el vehículo
	Monitoreo ambiental para la detecciòn de emergencias, desastres	Acceso a internet usando la www (World Wide Web)	Seguridad vial y control de tráfico
	Telemática	Sistema de Georeferenciación Vehicular	Eficiencia del tráfico
	Google Health	Control del tráfico ferroviario	Entretenimiento y servicios de información

	Microsoft Health Vault	Telealarma	Servicio e-call para aviso de concurrencia de accidentes en la vía.
	Agricultura y control de riego	Telemetría	Acceso a servicios de VoIP y vídeo bajo demanda desde el vehículo
	Observación de la tierra	Aplicaciones basadas en localización - Navegación, las condiciones del tráfico, horarios de avión / tren y buscador de ubicaciones	Aplicaciones de información y entretenimiento para los pasajeros del vehículo
	Transporte y tráfico de vehículos	Aplicaciones verticales - entrega de mercancías, gestión de flotas y automatización de la fuerza de ventas	Obtener información enriquecida de localización para mejora de eficacia de sistemas GPS.

De la comparación desarrollada en la Tabla 5, se deduce que la tecnología sensor cloud es idónea para la aplicación en monitoreo vehicular, debido a la capacidad de cómputo de datos, además de las características de almacenamiento en la nube que ofrece.

En relación a la tecnología GPRS, se considera como una tecnología complementaria a sensor cloud, la cual de ser implementada en el dispositivo Gateway, permitiría tener un rango de cobertura para monitoreo determinado por la infraestructura celular.

Las redes VANETS son idóneas para aplicaciones vehiculares debido a que cubren los requisitos de movilidad de los entornos vehiculares, sin embargo no posee la capacidad de cómputo apropiada para procesamiento y el almacenamiento es local, no ilimitado como en el caso de la nube.

En referencia a la tecnología sensor cloud, al estar formada por una red WSN y Cloud Computing, los estándares y protocolos que aplican son los correspondientes a ambas

tecnologías por lo cual su implementación tendría ventajas de ambas aplicaciones, así mismo en los temas de velocidad y transferencia de datos.

CAPITULO IV

PROPUESTA: Diseño de la red sensor cloud aplicada en prevención de accidentes de tránsito

En este capítulo se presenta el diseño de una red con tecnología Sensor Cloud aplicada en la prevención de accidentes de tránsito, se decriben sus componentes y se plantea el diseño de la infraestructura de red, conexiones y explicación de sus protocolos y funcionamiento y los mecanismos de seguridad respectivos.

A continuación el esquema propuesto de la arquitectura sensor cloud:

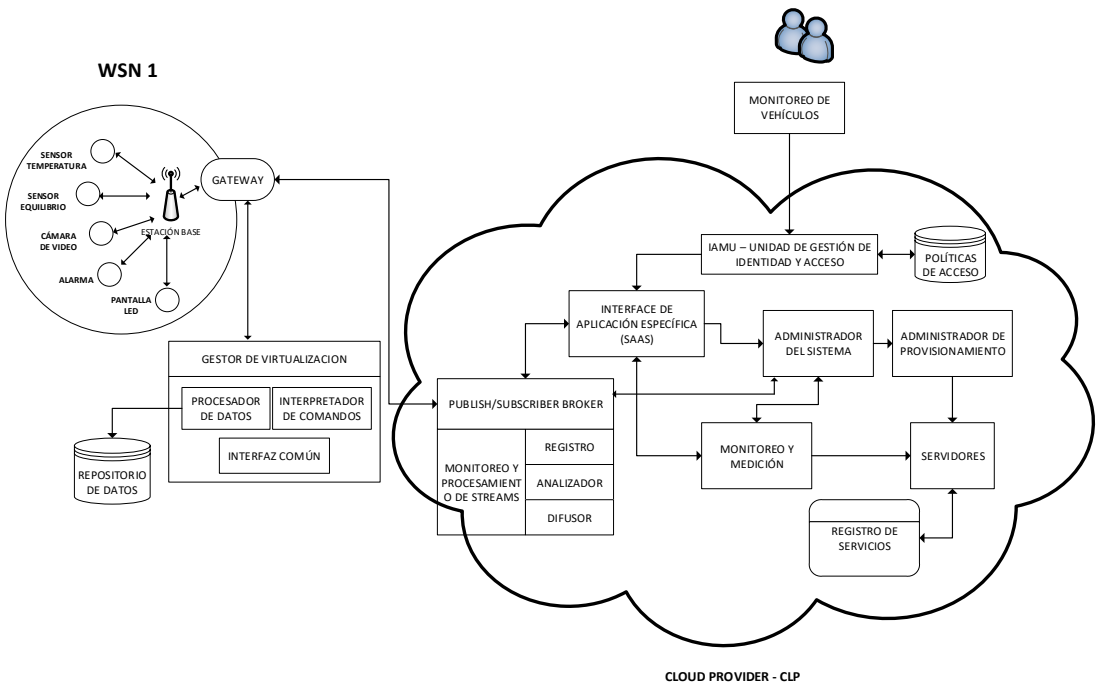


Figura 54. Arquitectura Sensor Cloud aplicada en prevención de accidentes de tránsito.

4.1Componentes de la arquitectura:

La arquitectura propuesta comprende los siguientes componentes:

4.1.1 Plataforma de sensores WSN (infraestructura de sensores inalámbricos)

La red de sensores inalámbricos WSN puede ser una arquitectura de sensores con radios de baja potencia, para lo cual se requiere un gateway que permita conectarse a una red IP, o la arquitectura de sensores puede incorporar una tecnología con conectividad IP directamente, estilo WIFI o red celular 2G, 3G, 4G, LTE.

Dependiendo de la arquitectura de la red WSN, se emplearían las siguientes tecnologías o protocolos de comunicación para el envío de datos desde la estación base o coordinador de la WSN al gateway: ZIGBEE, 6LOWPAN, dichas tecnologías están basadas en el protocolo IEEE 802.15.4 para la comunicación; luego el Gateway permitirá la conexión al entorno cloud computing; dependiendo del protocolo que se utilice estará determinada la cobertura de la comunicación. El Gateway está habilitado para recibir los datos capturados por los sensores y transferirlos a la plataforma de la nube en el internet usando un canal seguro.

En el diseño propuesto**,** la plataforma WSN se compone de los siguientes sensores: sensor de temperatura, sensor de mercurio o de equilibrio, cámara de video, los cuales se encuentran instalados en el vehículo, además se instalan algunos actuadores que servirán como mecanismos de alarma para el conductor y los pasajeros del vehiculo, entre ellos una alarma sonora y una pantalla led para indicación de mensajes. La alimentación de energía de los sensores se realiza a través de la batería del vehículo.

Los sensores inalámbricos del vehículo se conectan a la estación base (compatible con el estándar IEEE 802.15.4) y posteriormente a un módulo gateway, el cual recoge los datos de los sensores y transmite estos datos a través de canales de comunicación inalámbrica, puede ser la red celular (GPRS, 3G, 4G) a la plataforma de la nube

(entorno de nube) en internet usando un canal seguro SSL. Los sensores transmiten datos en tiempo real a la aplicación en la nube (aplicación SaaS) de forma continua basados en el tiempo de retardo que se ajusta en su programa de configuración.

Los datos obtenidos de la cámara de video, los cuales se envían a la plataforma en la nube, son procesados posteriormente con la capacidad computacional necesaria en la nube para determinar el estado emocional del conductor mediante: un algoritmo de detección corporal y facial para la inferencia de emociones mediante la visión por computador (Rey, 2012) o mediante la plataforma Emotions que ofrece estas funcionalidades, luego se emplea un algoritmo para determinar las acciones a realizarse en el vehículo para optimización de la seguridad vial.

En el modelo propuesto cada red WSN transmite los datos recolectados a la estación base usando una estructura de datos plataforma-independiente, el cual recibe la informaciòn a través de una interface Wireless y reenvía esto al Gateway por medio de una interface apropiada. El Gateway, a su vez extrae y encapsula la informaciòn en un formato específico (por ejemplo JSON**)** y envía todo ello al respectivo topico definido en el ambiente de cloud computing.

La aplicación en el Gateway realiza dos procesos: recibe informaciòn de la interface, extrae la informaciòn sensada contenida en la estructura de datos plataforma-independiente y pone tal información en un formato específico según el lenguaje de programación que se utilice en el desarrollo (por ejemplo JSON), el otro proceso que realiza el Gateway es establecer un canal de comunicación via HTTP con la plataforma cloud computing y los datos son enviados al módulo de publicación/ suscripción propuesta luego de pasar por el proceso de virtualización en el módulo Virtualization Manager.

A continuación se describen las funcionalidades de los diferentes componentes del modelo propuesto sensor cloud:

4.1.2 Gestor de virtualización

Este componente ayuda en la agregación de recursos autónomos y heterogéneos, es decir, recursos que serán usados por la plataforma.

Las redes de sensores inalámbricas son conectadas por el gateway a través de una interface común en diferentes formas (serial, usb y ethernet). El gateway recibe los datos en bruto de los puertos de comunicación y los convierte en un paquete. El paquete es guardado en un buffer para más procesamiento. El procesador de datos recupera los paquetes del búffer y lo procesa de acuerdo al tipo de paquete. El tipo de paquete depende de la aplicación que esté corriendo en la plataforma

El intérprete de comandos es el responsable de proveer el canal de comunicación reversa hacia el canal del gateway a la WSN. Este procesa e interpreta varios comandos emitidos por diferentes aplicaciones y genera el código que se entiende por los nodos sensores.

4.1.3 Publish/ subscriber broker- agente de publicación/ suscripción

Este módulo se encarga de la supervisión, el procesamiento y la entrega de los eventos a los usuarios registrados a través de aplicaciones de servicio (SaaS). Los cuatro componentes propuestos en este modelo son:

4.1.3.1 Monitoreo y procesamiento de streams (SMP):

Desde el agente de publicación/ suscripción llega al módulo SMP el flujo de sensores en muchas formas diferentes, en algunos casos se trata de datos en bruto que deben ser capturados, filtrados y analizados en tiempo real y en otros casos se almacena o se guarda en caché (stored or cached). El estilo de cálculo requerido depende de la naturaleza de los streams de datos (flujos). Por lo tanto, el componente SMP que se ejecuta en la nube supervisa los flujos de eventos (tramas o streams de sensores) e invoca el método de análisis correcto**,** en el caso de los datos de los sensores del vehículo el método correcto de análisis depende de la funcionalidad programada en el servidor web de acuerdo a la aplicación web. Este método permite por ejemplo en el caso de los datos que se obtienen de la cámara ejecutar el algoritmo que permita la determinación de las emociones del conductor.

Además en este módulo se ejecuta el modelo de ejecución paralelo en cloud, el cual permite que los datos de los sensores estén disponibles al mismo tiempo para diferentes usuarios de la plataforma, y se logra mediante la implementación en el desarrollo de la aplicación de un modelo de programación como **MapReduce**, el cual para realizar el procesamiento paralelo de grandes volúmenes de datos divide el trabajo en un grupo de tareas independientes, este estilo de programación es soportado pr algunas nubes.

4.1.3.2 Registry Component (RC)- Componente de Registro (RC):

Para el diseño propuesto, la aplicación SaaS correspondiente al control y monitoreo de vehículos se registra en el pub/ sub broker para la obtención de diversos datos de

sensores requeridos por la **entidad de seguridad o monitoreo vial** (usuario de la comunidad). Para cada aplicación, el **componente de registro** almacena las suscripciones de usuarios de esa aplicación y los tipos de datos de los sensores (temperatura, cámara de video, presión, etc.) a los que está interesada la aplicación. Además el componente de registro envía todas las suscripciones de usuario junto con el identificador de aplicación (application id) al componente de difusión (disseminator component) para la entrega de eventos.

4.1.3.3 Analyzer Component (AC) Componente Analizador

Cuando los datos o eventos de los sensores del vehículo llegan al agente de publicación/ subscripción (pub/sub broker), el componente analizador (analyzer component) determina a qué aplicaciones pertenecen y si necesitan una entrega periódica o de emergencia. Los eventos se pasan luego al componente de difusión (disseminator component) para entregar a los usuarios (entidad de control y monitoreo vial) apropiados a través de aplicaciones SaaS.

4.1.3.4 Disseminator Component (DC) Componente diseminador o difusor:

Para la aplicación SaaS de control y monitoreo vial, este componente difunde datos o eventos de sensores a usuarios suscritos (son los que requieren datos de los sensores por ejemplo la entidad de control y monitoreo vial) usando un algoritmo de coincidencia de eventos**.** Se puede utilizar el modelo de ejecución paralelo de Cloud para la entrega rápida de eventos.

Seguidamente se entrega los datos a través de la interfaz de aplicación al suscriptor o abonado.

4.1.4 Interface de aplicación específica:

En este proyecto se propone SaaS como la interfaz de aplicación específica. SaaS es la plataforma de cloud computing **Software as a Service** que combina datos y aplicaciones en conjunto y se ejecuta en el servidor Cloud, esta interfaz brinda flexibilidad a la entidad de control y monitoreo vial para acceder a los servicios de sensor cloud alojados remotamente a través de Internet.

La infraestructura de Cloud Computing SaaS que se propone está formada por un conjunto de máquinas de hardware de alto rendimiento, una infraestructura de redes de comunicación de datos para la conexión entre las máquinas clientes (entidad de control, monitoreo y seguridad vial y las máquinas remotas de alto rendimiento) y componentes de software: middleware de alto nivel, mecanismos de razonamiento y bases de datos.

4.1.5 Funcionamiento del algoritmo de la aplicación (SAAS)

Los procedimientos de minería de datos son responsables de crear las decisiones adecuadas en función de tres parámetros que son **identificación del conductor, tipo de sensor, y datos del sensor actuales.**

Cuando la aplicación recibe los datos de los sensores, el algoritmo comprueba si los datos del sensor están normal o anormal (a partir de los rangos normales de pruebas médicas de laboratorio y política médica del conductor que son definidas en el sistema),

y además ejecuta el proceso de detección de las emociones a partir de los datos obtenidos de la cámara de video.

Si los datos son normales, el algoritmo almacena estos datos en tablas de información de los sensores en la base de datos para rellenar los datos históricos de los conductores. De lo contrario, el algoritmo va a crear una decisión basado en un histórico de datos del conductor, que por lo general permitirá ejecutar una acción de retorno hacia el vehículo para mostrar una alarma en la pantalla y que el conductor tome las medidas de descanso necesarias para no exponer su vida ni la de sus pasajeros.

Si el conductor no tiene ningún dato histórico para la misma condición, el sistema tomará una decisión basado en los datos estadísticos históricos de los conductores que tienen una condición similar.

La plataforma de la nube (SaaS) debe tener los siguientes servicios:

1. Servicio de almacenamiento, que se encarga de almacenar los datos de los sensores.

2. Servicio de minería de datos, que es responsable de proporcionar decisiones basadas en los datos históricos de los conductores.

3. Servicio de gestión o monitoreo para actualizar, revisar y probar los datos de los conductores que se necesita por el personal de monitoreo vehicular. El personal de monitoreo vehicular y los conductores pueden utilizar la aplicación de diferentes dispositivos móviles y estacionarios conectados a Internet.

4.1.6 System Manager - Administrador del sistema (SM)

Este componente en el modelo propuesto es responsable de procesar, archivar los datos del sensor, y gestionar los recursos del sistema, así como el almacenamiento de los datos del sensor; por medio de los ciclos computacionales se procesan los datos que emiten los sensores. Gestiona los recursos (hardware y software) de la computadora o los servidores.

Además crea solicitudes de servicio sobre la base de la solicitud del usuario (entidad de monitoreo vial) para permitir el acceso a los datos almacenados en el **DR (Data Repository)** o para poner en el **DR (Data Repository)** los datos recogidos de una WSN. Las **solicitudes de servicio** se pasan al System Manager que unificará la solicitud y enviará esta solicitud al **pub/ sub broker** para encontrar una **asignación con un índice de datos** que se almacena en el **registro del agente de publicación/ suscripción.**

Cuando los datos de los sensores llegan al agente de publicación/ subscripción el administrador del sistema (System Manager) toma decisiones para los procesos de almacenamiento.

4.1.7 Monitoring and Metering - Monitoreo y Medición MaM:

Este módulo rastrea el uso de los recursos de la nube primaria, así como los recursos de los CLP (cloud providers) colaboradores para que los recursos utilizados puedan atribuirse a un usuario determinado.

4.1.8 Registro de servicios:

En el modelo propuesto el registro de servicios se encarga de descubrir y almacenar información de recursos y políticas en el dominio local. Los recursos de hardware y software además de las políticas que se manejen.

4.1.9 Unidad de gestión de identidad y acceso IAMU

Cuando el usuario o entidad de seguridad vial requiere información de la plataforma Sensor Cloud, se conecta a la aplicación específica SaaS a través de la IAMU, la cual se encarga de proporcionar autenticación entre el cliente **(entidad de monitoreo y seguridad vial)** y el proveedor **(aplicación SaaS)**, además de proporcionar a los recursos de la nube un control de acceso basado en políticas, como mecanismos de seguridad.

La ACDU **Unidad de Control de Acceso de Aplicación** autentica al usuario mediante un mecanismo o proceso de interacción en el cual el Edge Node (implementa Kerberos y su algoritmo de clave pública Diffie Hellman), recibe la solicitud del usuario y la envía al servidor de autenticación, el cual, en base a las políticas de acceso asocia a los usuarios con directivas de acceso y, una vez completado este proceso, el usuario obtiene acceso a los recursos de datos dentro de las limitaciones impuestas por las políticas de acceso. El modelo propuesto incluye control, gestión de grupos y usuarios y otra información que se almacena utilizando XML.

4.1.10 Servidores web de la arquitectura

Los servidores web son responsables de almacenar el contenido y entregarlos de forma fiable. La estructura de un servidor se divide en dos capas: superposición y núcleo. En la capa de superposición, un servidor comprende un host de servicio web (por ejemplo, Apache o Tomcat), un agente de política y un asignador de SLA (Acuerdo de Nivel de Servicio). El host de servicios web garantiza la entrega de contenido a los usuarios

finales sobre la base de las políticas negociadas. El agente de la política es responsable (junto con el mediador) para determinar qué recursos se pueden delegar y bajo qué condiciones se permite la delegación de políticas. El asignador de SLA realiza el aprovisionamiento y la reserva de los recursos del servidor Web (por ejemplo, CPU, ancho de banda, almacenamiento, etc.) para satisfacer los SLA locales y delegados y garantiza que se aplican los términos de los SLA. El núcleo del servidor web consta de sistemas de computación de alto rendimiento, como multiprocesadores simétricos, sistemas de clúster u otros sistemas empresariales. Los algoritmos subyacentes de los servidores Web realizan el caché bajo demanda, la selección de contenido y el enrutamiento entre servidores. Esto requiere que cada servidor Web exprese sus propias políticas de almacenamiento y administración de contenido.

4.1.11 Funcionamiento del modelo de la arquitectura propuesta sensor cloud

1. La red inalámbrica de sensores se conecta a través de la estación base o coordinador al gateway a través de una interfaz común y un protocolo de comunicaciones basado en **IEEE 802.15.4** de diferentes maneras.
2. El Gateway recibe los datos sin procesar de los puertos de comunicación y los convierte en un paquete. El paquete se mantiene en un búfer para procesamiento posterior.
3. En el módulo **Virtualization Manager**, el procesador de datos (Data Processor) recupera los paquetes del buffer y procesa según su tipo. El tipo de paquete depende de la aplicación que se ejecute en la plataforma, la aplicación propuesta de control y monitoreo vial es SaaS. Los datos se procesan en un formato de almacenamiento y luego se envían al Repositorio de Datos **(Data Repository DR)**.

4. El intérprete de comandos proporciona el canal de comunicación inversa desde el gateway a la red de sensores inalámbricos (WSN), El cual se encarga de procesar e interpretar varios comandos emitidos por diferentes aplicaciones y genera el código que es comprendido por los nodos del sensor para las acciones a realizarse por los nodos actuadores de la WSN.
5. Enseguida los datos de los sensores del vehículo llegan al agente de publicación/ subscripción, que se encarga de brindar las capacidades necesarias para que varias aplicaciones puedan acceder a los mismos datos de sensor (ejecución paralela).
6. Al componente **Stream Monitoring and Processing** llega el flujo de sensores de muchas maneras diferentes, en algunos casos se trata de datos en bruto que deben ser capturados, filtrados y analizados en tiempo real y en otros casos se almacena o en caché. El estilo de cálculo depende de la naturaleza de los streams. Por lo tanto SMPC que se ejecuta en la nube, supervisa los flujos de eventos e invoca el método correcto de análisis. Dependiendo de las velocidades de datos y la cantidad de procesamiento que se requiere; además SMP gestiona el modelo de ejecución paralelo en Cloud.
7. Las diversas aplicaciones SaaS se registran en el agente de publicación/ subscripción para diversos datos requeridos por el usuario de la comunidad. Para cada aplicación el **Componente de Registro** almacena las suscripciones de usuario de esa aplicación y los tipos de datos del sensor (temperatura, luz, presión, etc) a los que está interesada la aplicación. También envía todas las suscripciones de usuario junto con el identificador de aplicación (application ID) al componente de Difusión **(Disseminator component)** para la entrega de eventos.

8. Cuando los datos o eventos del sensor llegan al agente de publicación/ subscripción, el componente analizador (**analyzer component**) determina a que aplicaciones pertenecen y si necesitan una entrega periódica o de emergencia. Luego los eventos se pasan al componente de difusión **(disseminator component)** para entregar a los usuarios apropiados a través de aplicaciones SaaS.
9. El componente de difusión (**disseminator component**) mediante el algoritmo de coincidencia de eventos, encuentra los abonados (suscriptores) apropiados para cada aplicación SaaS y entrega los eventos. Se puede usar el modelo de ejecución paralelo de cloud para la entrega rápida de eventos.
10. Los ciclos computacionales son proporcionados internamente por el **SM (System Manager)** según sea necesario para procesar los datos emanados de los sensores. El SR **(Service Registry)** administra las suscripciones y credenciales de usuario.
11. **MaM (Monitoring and Metering)** calcula el precio de los servicios ofrecidos.

4.2 Características y funcionalidades del diseño sensor cloud para control y monitoreo vial.

1. La aplicación SaaS puede desarrollarse como una aplicacion web que permite llevar a cabo la gestión de la arquitectura, administrar el repositorio de reglas y eventos, realizar el control de los usuarios, mantener los servicios y definir la relación entre las aplicaciones basadas en reglas y las fuentes de datos. Por lo tanto, las aplicaciones de dominio pueden consumir datos de las fuentes de datos que les interesan. La interfaz de usuario de la aplicación debe

proporcionar acceso a varios elementos de la arquitectura prototipo. Por ejemplo, debe ser posible crear, editar y eliminar usuarios, definir perfiles de acceso, crear, editar y borrar archivos del repositorio de reglas, y definir los usuarios que tienen acceso al estado de desarrollador, y que redes de sensores inalámbricos quieren consumir datos. También debe ser posible la creación, edición y eliminación de los servicios.

2. Los servicios web pueden desarrollarse bajo una arquitectura de servicios web RESTful**,** obteniendo bajo acoplamiento y habilitando el desarrollo de nuevos servicios para ser utilizados por los usuarios. Los servicios Web de la plataforma sensor cloud tienen acceso a través de las interfaces construidas con tecnologías Web 2.0.

3. El diseño propuesto emplea un esquema de **publicación/ suscripción**, en el cual los suscriptores proporcionan solicitudes de información al sistema y los editores envían nueva información al sistema. Al recibir una publicación, el sistema busca suscripciones coincidentes y notifica a los suscriptores interesados. Este modelo reduce la complejidad del programa y el consumo de recursos.

4. El modelo de publicación/ suscripción puede basarse en contenido, lo que simplifica la integración de la red de sensores con aplicaciones céntricas centradas en la nube (comunity-centric cloud).

5. El agente de publicación/ subscripción (pub/ sub broker) ejecuta el algoritmo de coincidencia de eventos, el cual sirve para entregar los datos o eventos de los sensores publicados a los suscriptores. Especificamente el componente difusor (disseminator) del pub/sub broker utiliza o ejecuta el algoritmo de coincidencia de eventos, mediante el cual encuentra los suscriptores adecuados para cada aplicación y entrega los eventos para su uso.

6. Se puede implementar el **algoritmo de coincidencia de eventos** "Statistical Group Index Matching/ Comparación de índices de grupos estadísticos (SGIM)", el cual es un algoritmo de coincidencia de eventos rápido y escalable, que permite la entrega de los datos o eventos de los sensores publicados a los usuarios apropiados de las aplicaciones cloud que han sido suscritas, es necesario que coincidan los eventos publicados con las suscripciones de manera eficiente.

7. Es posible que una enorme cantidad de datos de sensores pueda ser capturada y transmitida, por lo que es importante contar con un mecanismo para recibir los datos y enviarlos a las aplicaciones que han hecho las suscripciones necesarias. En este trabajo, se puede adoptar el **modelo de gestión de colas.** Las colas pueden ser entendidas como los suscriptores de los que se tiene interés en recibir datos. Cada aplicación tiene una cola. Las colas de mensajes surgen a medida que las notificaciones de los temas con los datos llegan de las fuentes de datos. Un hilo de ejecución (thread) consume o procesa mensajes a medida que llegan a la cola. Este hilo recibe el **JSON** (Java Script Object Notation) y lo transforma en un objeto Java. El formato JSON es un lenguaje de programación

alternativo a XML, que se considera una opción con la cual se programarían las funciones necesarias en el servidor web.

8. En referencia al modelo de programación, se puede utilizar **MapReduce**, que es adecuado para soluciones de bases de datos distribuidas es decir con almacenamiento distribuido. MapReduce puede utilizarse para almacenar y analizar datos de sensores y se puede utilizar en el desarrollo del marco de Cloud Computing propuesto para WSN. Mediante MapReduce se puede diseñar un esquema de base de datos para incluir una colección de tablas para almacenar lecturas de sensores individuales y para proporcionar enlaces a lecturas de sensores relacionadas. El modelo propuesto también puede incluir una metodología para analizar y modelar datos de sensores y varias estadísticas especiales de interés tales como la localización del sensor, el tipo y propósito de la red de sensores, los datos recolectados y otra información global asociada. EN el modelo propuesto se puede utilizar principios de almacenamiento distribuido y la introducción de **MapReduce** dentro del régimen de almacenamiento de datos permite un mejor almacenamiento y recuperación de datos a través de los sistemas distribuidos.

9. La Gestión de la información en WSN puede realizarse mediante TINY DB por ser ésta la más avanzada en cuanto a abstracción en el manejo de datos en el entorno. TinyDB es un sistema de procesamiento de consultas para extraer información de una red de sensores. Proporciona una interfaz similar a SQL y permite trabajar con consultas contra la red de sensores inalámbricos como si

se tratara de una base de datos tradicional. Además, TinyDB implementa varias optimizaciones para manejar los datos eficientemente.

10. En el caso del Gateway, se puede utilizar un módulo Raspberry Pi, que permite una comunicación directa por USB a un módulo Arduino que actuaría como nodo coordinador de una red inalámbrica, así como facilita la construcción de una interfaz gráfica para el usuario (ofrecida por ejemplo directamente en un monitor conectado, por red mediante un servidor http, etc...), o la comunicación con un servidor externo a través de Internet.

11. Si el proveedor de cloud CLP no posee la capacidad para manejar parte de la carga de trabajo en sus servidores web, se puede añadir al diseño un esquema de organización virtual basado en colaboración dinámica, el cual sería gestionado por los componentes: Mediador, Agente Colaborador, Policy Repository.

4.3 Seguridad en el modelo sensor cloud propuesto

La seguridad y la privacidad son factores significativos relacionados con el entorno de nube. El entorno de cloud computing ofrece numerosos recursos de computación que se comparten. Por lo tanto, comparten recursos de hardware y áreas de almacenamiento de datos en la nube por lo que están expuestos a información privilegiada y/o ataques de afuera.

1. Para lograr seguridad y privacidad en el diseño propuesto se aplica la técnica **Secure Socket Layer (SSL),** que es una técnica popular para el establecimiento de un canal cifrado entre un **servidor web y el Gateway** para transmitir los datos de los conductores para la aplicación en la nube a través de canales seguros.
2. El sistema se encarga de encriptar los datos antes de almacenarlos en la nube, diferentes tipos de algoritmos de cifrado se han desarrollado para proporcionar a los usuarios de la nube con la seguridad de los datos. El objetivo de estos algoritmos es proteger el sistema contra usuarios maliciosos y proteger la información contra las amenazas avanzadas.
3. En este diseño se propone el algoritmo simétrico Advanced Encryption Standard (AES). Los datos serán almacenados en la nube utilizando este formato.

4.4 Ventajas del diseño propuesto

Hay varias ventajas para el sistema propuesto, incluyendo:

1. Proporcionar la recolección de datos en tiempo real.

2. La eliminación manual del proceso de recolección de datos, que incluye algún momento los errores de entrada de datos.

3. Hacer posible el seguimiento de un gran número de conductores que dependen de un número limitado de personal de monitoreo, y que trabajan todo el día sin periodos de descanso lo cual puede afectar su desempeño y puede provocar accidentes. El monitoreo constante permite disminuir los riesgos de accidentes por medio del envío de alarmas.

4. Asegurarse de que no existan accidentes que sean causados por problemas de estrés del conductor.

5. En una infraestructura sensor cloud, a diferencia de las redes de sensores que normalmente son utilizadas para aplicaciones con objetivos específicos; la información obtenida de diferentes sensores puede ser compartida y utilizada por múltiples aplicaciones, lo cual se logra al virtualizar los diversos nodos de una red en una plataforma en la nube.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- La tecnología Sensor Cloud consiste en la integración entre Wireless Sensor Network (WSN) y Cloud Computing, lo cual permite ejecutar el procesamiento de datos y almacenamiento en la nube, por lo que existe una baja latencia y flexibilidad, además se puede acceder a los datos desde todo el mundo.

- El diseño de la infraestructura sensor cloud aplicada en prevención de accidentes de tránsito propuesta permite el intercambio de datos de sensores de los vehículos en tiempo real a través de Cloud Computing; para resolver los problemas de seguridad en la nube se propone IAMU (Identity and Access Management Unit), un módulo de identidad y control de acceso que permitirá brindar seguridad al sistema mediante la gestión por medio de un repositorio de políticas definidas por el usuario de la infraestructura. El esquema que se propone es de publicación/ suscripción y la interfaz de aplicación específica es de tipo SaaS, lo que deja abierta la posibilidad de plantearse la plataforma web sea bajo el estilo SOAP o REST.

- En la arquitectura propuesta se plantea un módulo Gateway como interfaz WSN-Cloud, el cual permite resolver el problema de interconexión de la red de sensores inalámbricos WSN que se encuentra en el vehículo con el protocolo TCP/IP que se requiere para el envío y almacenamiento de la información en la

nube; actualmente existen un sin número de módulos que pueden desempeñar tales funciones.

- La integración de WSN y Cloud computing simplifica la operación y mantenimiento del sistema, además el procesamiento común, computacional y tareas analíticas se pueden alojar en servicios en la nube con lo cual se logra liberar a los dispositivos sensores de ejecutar aplicaciones pesadas que consumen muchos recursos y por lo tanto se reduce el consumo de energía y se maximiza la vida útil de las unidades de energía, así como de la propia red.

- La red de sensores inalámbrica WSN está formada por nodos o sensores que pueden tener características para conexión con redes IP o no, en el modelo propuesto, si los sensores tienen conectividad IP, la información se envía directamente sin necesidad de un gateway, caso contrario se necesita un gateway para que realice la conección de los sensores, los módulos gateway están disponibles en el mercado en diferentes tamaños y con capacidades de manejar un protocolo de comunicación específico.

- En la presente investigación se analizó las tecnologías GPRS y VANET como potenciales para el desarrollo de aplicaciones vehiculares, GPRS tiene conexión permanente a las redes de datos y existen varios dispositivos con esta tecnología adaptados para la conexión a un vehículo y monitoreo de variables. Las redes VANET tienen una capacidad amplia de comunicación con diferentes tecnologías como GPRS, lo cual evidencia la amplia cobertura que tendrá en el futuro, las dos tecnologías analizadas son complementarias en aplicaciones

vehiculares, así mismo la tecnología sensor cloud puede implementar GPRS para la comunicación desde los módulos gateways.

- El diseño de infraestructura sensor cloud propuesto puede ser usado como base para otras aplicaciones como en el campo de la salud, la videovigilancia, telemedicina y toda actividad que requiera de monitoreo de variables.

- En referencia a los temas de seguridad en el servidor web se pueden implementar algunas mejoras como: activar el puerto HTTPS para cifrar el tràfico web en caso de que alguien espíe la red, cerrar todos los puertos que puedan suponer un problema en el caso de un ataque malicioso, configurar el cortafuegos que se puede instalar para tratar todo el tráfico entrante y saliente, crear un sistema de usuarios y permisos para limitar el acceso a determinadas partes.

5.2 Recomendaciones

- Actualmente se están desarrollando un sin número de algoritmos y aplicaciones para la detección de emociones, así como también hay nuevo desarrollo en sensores, por lo que las aplicaciones pueden ser mejoradas y permitirán la optimización de recursos debido a que en los propios nodos de la red WSN se dotará de procesamiento, acelerando así el proceso de comunicación.

- La tecnología sensor cloud se encuentra en desarrollo por lo que aún se requiere de protocolos y estándares específicos que pemitan su mejor implementación

en los sistemas actuales, la tecnología sensor cloud apunta a la interacción con sensores móviles.

- Una plataforma sensor cloud, la cual está formada por cloud computing es vulnerable a problemas de seguridad, por tal razón es recomendable agregar las características necesarias para proveer de seguridad al sistema dependiendo de la aplicación que se requiera implementar.

- Las redes de sensores y el gateway pueden ser implementados mediante el uso de hardware libre, sin embargo, para la implementación de estos sistemas en nuestro país resulta costosa la inversión por temas de importaciones y pagos de aranceles; con fines de investigación y desarrollo de nuevos sistemas que aporten al desarrollo de nuevos sistemas en el Ecuador se debería exonerar de estos valores.

GLOSARIO

6LOWPAN	Estándar que posibilita el uso de IPv6 sobre redes basadas en el estándar IEEE 802.15.4.
CLOUD COMPUTING	Es un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet.
GATEWAY	Puede referirse a un nodo en una red que sirve de punto de acceso a otra red.
GPRS	El servicio general de paquetes vía radio es una extensión del "Sistema Global para comunicaciones Móviles" (Global System for Mobile Communications o GSM) para la transmisión de datos mediante conmutación de paquetes.
HADOOP	es un sistema de código abierto que se utiliza para almacenar, procesar y analizar grandes volúmenes de datos. Aísla a los desarrolladores de todas las dificultades presentes en la programación paralela.
HBASE	Es una base de datos NoSQL de código abierto.
HTML	Lenguaje utilizado para la creción de documentos de hipertexto e hipermedia. Es el estándar usado en el world wide web.
IEEE 802.15.4	Estándar que define el nivel físico y el control de acceso al medio de redes inalámbricas de área personal con tasas bajas de transmisión de datos (low-rate wireless personal area network, LR-WPAN).
IPV6	Protocolo de Internet versión 6, definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol version 4.
JSON	Acrónimo de JavaScript Object Notation, es un formato de texto ligero para el intercambio de datos, se considera un formato de lenguaje independiente, alternativo a XML.
MAP REDUCE	Modelo de programación para dar soporte a la computación paralela sobre grandes colecciones de datos en grupos de computadoras.

RASPBERRY PI	computador de placa única o computador de placa simple (SBC) de bajo coste, el software que implementa es open source.
REST	Estilo de arquitectura software para sistemas hipermedia distribuidos como la World Wide Web. Permite diseñar sistemas de servicios web.
SAAS	Software as a Service es un modelo de distribución de software donde el software y los datos se alojan en servidores a los cuales se accede vía internet desde un cliente.
SOAP	Simple Object Access Protocol) es un protocolo estándar que define cómo dos objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML, es usado en los servicios web.
TINYOS	sistema operativo de código abierto basado en componentes para redes de sensores inalámbricas. . Está diseñado para incorporar novedades rápidamente y para funcionar bajo las importantes restricciones de memoria que se dan en las redes de sensores.
VANET	Una red ad-hoc vehicular es un tipo de red de comunicación que utiliza a los vehículos como nodos de la red.
WAVE	Wireless Access in Vehicular Environments es la estandarización de un grupo de protocolos de acceso inalámbrico en entornos vehiculares llevada a cabo por un grupo de trabajo del IEEE. El objetivo principal de WAVE, es proporcionar comunicación ya sea V2V (vehículo a vehículo), como V2I (vehículo a infraestructura)
WEB	Red informática, Internet
WSN	Wireless Sensor Network, red de nodos equipados con sensores, que colaboran en una tarea común.
XML	"Lenguaje de Marcas Extensible", meta-lenguaje que permite definir lenguajes de marcas desarrollado por el World Wide Web Consortium (W3C) utilizado para almacenar datos en forma legible.

Bibliografía

Adriana Cornejo, C. D. (2015). Análisis, Diseño e Implementación de Cloud Computing para una Red de Voz sobre IP. CUENCA.

Agencia Nacional de Regulación y Control del Transporte Terrestre, T. y. (2015). Proyecto Seguridad Integral para el Transporte Público y Comercial,. Ecuador.

Alejandro Cama, E. D. (Octubre de 2012). Las redes de sensores inalámbricos y el Internet de las cosas. *Revista INGE CUC, Volumen 8, Número 1*, 163-172.

Antoni Gabriel Caicedo Bastidas, J. M. (diciembre de 2011). Evaluación del Desempeño de Redes 802.11p/ WAVE en la Transmisión de Datos, Voz y Video IP. Cauca, Colombia: Grupo I+D Nuevas Tecnologías en Telecomunicaciones.

Baltrusaitis, T. (2014). Automatic facial expression analysis. Universidad de Cambridge.

Batista, M. E. (Mayo de 2012). Localización de roadside units en una red de transporte público para máxima probabilidad de comunicación. Santiago de Chile.

Beng, L. H. (13 de Abril de 2009). Sensor Cloud: Towards Sensor-Enabled Cloud Services. Intelligent Systems Center Nanyang Technological University.

Bocchio, F. (2014). Modelo Cloud Computing como Alternativa para Escalabilidad y Recuperación de Desastres. Buenos Aires: UTN.BA.

Carbajal, E. F. (2012). *Redes de sensores inalámbricas aplicada a la medicina.* Cantabria: Escuela Técnica Superior de Ingenieros Industriales y de Telecomunicación, Universidad de Cantabria.

Carlos Taffernaberry, A. D. (IETFDay 2015). Aplicaciones del RFC 4944 - 6lowPAN en IoT SIPIA6 - Red de Sensores Inalámbricos con IPv6. Mendoza: gridTICS – Grupo UTN de I&D en Tecnologías de la Información y las Comunicaciones.

Computing, M. s. (Abril de 2010). *Cloud Computing, una perspectiva para Colombia.*

Domínguez, F. J. (2010). Improving Vehicular ad hoc Network Protocols to Support Safety Applications in Realistic Scenarios. Valencia, España.

Donato, F. P. (2010). Transmisión de imágenes de video mediante servicios WEB XML sobre J2ME. Sevilla, España: Universidad de Sevilla.

Durán, E. I. (2015). Diseño y elaboración de un prototipo de monitor de signos vitales aplicando métodos no invasivos con comunicación de datos a dispositivos móviles. Cuenca: Universidad Politécnica Salesiana.

EMOTIENT. (2017). *Emotions Drive Spending, A New Age for Advertising Copy Testing Facial Expression Measurement Technology.* Obtenido de https://imotions.com/.

ESEC. (2014). Introducción a las Redes de Sensores Inalámbricas. España: Plataforma Tecnológica Española .

Fernando Paúl Espinoza Peñaherrera, A. F. (2009). Pago electrónico a través de teléfonos móviles. Guayaquil, Ecuador.

Franklin Silvio Córdova Ochoa, P. A. (2012). Diseño y construcción de un sistema de alarma y frenado automático para un vehículo al detectar conductores somnolientos.

Giraldo, M. A. (Mayo de 2013). Estudio y Simulación de Redes Ad-Hoc Vehiculares VANETS. Universidad Católica de Pereira Ingeniería de Sistemas y Telecomunicaciones.

Giuseppe Lo Re, D. P. (2014). Advances onto the Internet of Things: Urban Air Quality Monitoring Using Vehicular Sensor Networks. Warsaw, Poland: Springer-Polish Academy of Sciences.

Guerrero, M. (agosto de 2013). Estudio para implementar un sistema de georeferenciación vehicular con controles en velocidad y seguridad. Maestría en Redes de Comunicaciones, PUCE.

Hassan, M. M. (2009). A Framework of Sensor - Cloud Integration Opportunities and Challenges. South Korea: Dept. of Computer Engineering Kyung Hee University Seocheon, Giheung-gu, Yongin Gyeonggi-do, 446-701.

Héctor Ramos Morillo, F. M. (2010). Redes Inalámbricas de Sensores Inteligentes. Aplicación a la Monitorización de Variables Fisiológicas. *Universidad de Alicante*.

Hernandez, J. (2014). AUTOEMOTIVE, Bringing Empathy to the Driving Experience to Manage Stress,. MIT Media Lab.

Hernández, J. V. (2010). *Redes inalámbricas de sensores: una nueva arquitectura eficiente y robusta basada en jerarquía dinámica de grupos.* Valencia.

Ibañez, P. (25 de julio de 2011). *Sistemas de detección en los coches para evitar accidentes.* Obtenido de http://www.xataka.com/automovil/sistemas-de-deteccion-en-los-coches-para-evitar-accidentes,

IEEE. (2006). IEEE Standard for Local and metropolitan area networks, Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs),. *IEEE Std 802.15.4TM-2011*.

Jamal N. Al-Karaki, A. E. (s.f.). Routing Techniques in Wireless Sensor Networks: A Survey, . *Dept. of Electrical and Computer Engineering Iowa State University,*.

Javier Martínez Fernández, J. C. (Noviembre de 2012). A Sensor Technology Survey for a Stress-Aware Trading Process . IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS - PART C: APPLICATION.

Juan Carlos Amay Izquierdo, F. P. (Junio de 2014). Análisis, diseño e implementación de un sistema de alarma para el monitoreo del registro de la lluvia en la ciudad de Cuenca basado en el protocolo GPRS. Cuenca.

Juan G. Tamayo, L. S. (2013). Estudio, diseño e implementación de una red de datos con tecnología GPRS. Latacunga.

K. Surya Bharat, A. P. (2014). Sensor Information Management using Cloud Computing. *International Journal of Computer Applications*, Volume 103, No. 14.

K.Lakshmanarao. (2013). Survey on different issues of Sensor-Cloud. *International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 2 Issue 10*.

KelionBBC, L. (junio de 2014). *Crean dispositivo que detecta las emociones humanas a partir de la piel.* Obtenido de http://www.bbc.com/mundo/noticias/2014/06/140626_ciencia_monitor_piel_de_gallina_mz.shtml

Khandakar Entenam Unayes Ahmed, M. A. (2014). Integrating Wireless Sensor Networks with Cloud Computing . Melbourne, Australia: School of Electrical and Computer Engineering, RMIT University.

López, J. A. (2013). Contribución al diseño, definición e implementación de una plataforma de investigación para la Internet del Futuro, basada en un despliegue masivo de redes de sensores inalámbricos heterogéneos, en el marco de la Ciudad Inteligente. Universidad de Cantabria.

Lucas Iacon, P. G. (Julio de 2012). Estudio de la Integración entre WSN y redes TCP/IP. *Memoria de Trabajos de Difusión Científica y Técnica, núm. 10* .

Lucas Iacono, C. G. (2013). *Wireless Sensor Networks: A Software as a Service Approach.* Mendoza, Argentina.: Instituto de Microelectrónica, Facultad de Ingeniería, Universidad de Mendoza.

Lucas Iacono, C. G. (29-30 de July de 2013). Wireless Sensor Networks: A Software as a Service Approach. Mendoza, Argentina: Instituto de Microelectrónica, Facultad de Ingenierıa, Universidad de Mendoza.

Luis Alberto Caldas Calle, J. C. (Mayo de 2013). Implementación de un ambiente de simulación basado en software libre para el estudio de la provisión de servicios de comunicaciones en redes vehiculares ad-hoc mediante el uso de nodos móviles virtuales. Cuenca.

Luis, J. A. (2012). *Computacion en la nube. Estrategias de Cloud Computing en las empresas.* Alfaomega, .

Madoka Yuriyama, T. K. (2010). Sensor-Cloud Infrastructure, Physical Sensor Management with Virtualized Sensors on Cloud Computing, . Tokyo , Japan: IBM Research.

Mahmood, Z. (2014). *Cloud Computing, Challenges, Limitations and R&D Solutions.* South Africa: Springer.

Maldonado, V. (2012). Comparación de protocolos de enrutamiento y modelos de movilidad para Redes Ad-Hoc Vehiculares usando mapas reales. Loja, Ecuador.

Maya, E. (2014). *Red Inalámbrica de Sensores a través de 6LOWPAN para una agricultura de precisión aplicado en la hacienda Cananvalle de la ciudad de Ibarra.* Ibarra.

Microsoft. (2012). Cómputo en la nube, nuevo detonador para la competitividad de México. México: Publicación Instituto Mexicano para la competitividad.

Navarro, R. (Julio de 2006). Rest VS Web Services. Modelado, Diseño e Implementación de Servicios Web.

Niranjan Lal, S. Q. (2013). Detailed Dominant Approach Cloud Computing Integration with WSN. India: Institute of Hydropower Engineering & Technology Tehri (UK).

Novillo, C. (2014). Diseño e implementación de un sistema de seguridad con videocámaras, monitoreo y envío de mensajes de alertas a los usuarios a través de una aplicación web y/o vía celular. Universidad de Guayaquil, Facultad de Ciencias Matemáticas y Físicas.

ORSI, J. d. (s.f.). *Cloud Computing, La Tecnología como servicio.* Obtenido de https://sg.com.mx/content/view/674

Pérez, A. (Febrero de 2012). Implementación de tecnología de Cloud Computing para ofrecer servicios de infraestructura (IaaS) en la Facultad de Telemática. Colima.

Peter Mell, T. G. (2011). The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology . National Institute of Standards and Technology. Publication 800-145.

Quirasco, P. H. ((2007)). *Sistemas Telemáticos y las Organizaciones Inteligentes en la Sociedad del Conocimiento.* Universidad Veracruzana.

Rey, J. (2012). Universidad Carlos III Madrid, Inferencia de Emociones a través de Detección Corporal y Facial.

Roberto Fernández Martínez, J. O. (2009). *Redes inalámbricas de Sensores: Teoría y Aplicación Práctica.*

Roberto Fernández Martínez, J. O. (2009). *Redes inalámbricas de Sensores: Teoría y Aplicación Práctica.* España: Grupo de Investigación EDMANS - Universidad de la Rioja.

Rodríguez, J. (2006). Diseño de un sistema inalámbrico para el monitoreo en tiempo real de temperatura y humedad relativa bajo invernadero. *Universidad de la Salle, Facultad de Ingeniería de Diseño y Automatización Electrónica*. Bogotá d.c.

Saha, S. (2015). Secure Sensor Data Management Model in a Sensor Cloud Integration Environment. India: School of Mobile Computing and Comunications.

Saha, S. (2015). Secure Sensor Data Management Model in a Sensor Cloud Integration Environment . *(AIMoC), Applications and Innovations in Mobile Computing*.

Sajjad Hussain Shah. (2013). A New framework to Integrate Wireless Sensor Network with Cloud Computing. Pakistan: Departament of Computer Science,Bahria University.

Sánchez, J. A. (2005). Análisis y Estudio de Redes GPRS. Valdivia.

Sanjit Kumar Dash, J. P. (s.f.). Assimilation of Wireless Sensor Network and the Cloud. Odisha, India: Anusandhan University, Bhubaneswar, Institute for Computer.

Saymon Castro de Souza, J. G. (December de 2013). A Rule-Base Approach for WSN Application Development in a Cloud Environment. Journal of Advances in Computer Networks, Vol. 1, No. 4, .

Scanaill., M. J. (2013). Sensor Technologies, Healthcare, Wellness and Environmental Applications. Europa: Apress open.

Serrano, M. R. (2012). Inteligencia en comunicaciones entre vehículos. Leganés , Madrid: Ing. Telecomunicación Universidad Carlos III de Madrid,.

Shah, S. H. (2013). A New framework to Integrate Wireless Sensor Networks with Cloud Computing. Islamabad, Pakistan: Bahria University y ZSABIST.

Subarna Chatterjee, S. M. (2015). Optimal Composition of a Virtual Sensor for Efficient Virtualization Within Sensor-cloud. India: IEEE School of Information Technology Indian Institute of Technology Kharagpur, .

Subasish Mohapatra, B. M. (2014). The Scalable Architecture for Future Generation Computing Department of Computer Science and Engineering. *National Institute of Technology,* . India: Springer.

Tello, J. P. (Abril de 2012). Universidad Politécnica Salesiana Carrera de Ingeniería Electrónica, sistema de localización monitoreo y control vehicular basado en los protocolos GPS/GSM/GPRS. Cuenca.

Toutouh, J. (2013). Computación Natural en Redes Vehiculares. España: enguajes y Ciencias de la Computación Universidad de Malaga.

Tuñón, P. (8 de marzo de 2014). Sensores para detectar emociones. *Diario GIJÓN La Nueva España*, pág. 7.

Vallejo, S. Z. (2007). Diseño e implementación de un sistema de vigilancia remota para una residencia utilizando plataformas GPRS e Internet. Sangolqui, Ecuador.

Víctor Sandonís Consuegra, M. C. (julio de 2014). Conectando los vehículos a Internet en el sistema de transporte inteligente estandarizado por el ETSI. Departamento de Ingeniería Telemática, Leganés,.

Wasai Shadab Ansari, A. M. (2012). Survey on Sensor-Cloud: Architecture, Applications and Approaches. Chair of Mobile and Pervasive Computing, CoCIS, KSU Riyadh, KSA,.

Zach Shelby, C. B. (2010). 6LoWPAN, The Wireless Embeded Internet. TZI, Germany,: Universität Bremen.