Resumen

Actualmente los sistemas de transporte se utilizan con el propósito de desarrollar una gran variedad de actividades cotidianas como el traslado de bienes materiales, el transporte de personas, servicios de salud, entre otros. No por nada se considera que los vehículos se han vuelto una herramienta de gran importancia para las sociedades modernas e incluso han evolucionado a lo largo de la historia. En el presente trabajo nos centraremos en el uso del internet de las cosas aplicado a los vehículos el cual es conocido como IoV o Internet de los Vehículos.

Las nuevas tecnologías implementadas en los vehículos han permitido un avance gradual en su funcionamiento lo que permite que estos brinden mejores servicios y prestaciones [101]. Algunas tecnologías implican el desarrollo de nuevos materiales, la implementación de sistemas de entretenimiento, instalación de sistemas de soporte a bordo, sistemas de control más precisos y recientemente los sistemas de conducción autónoma. En la actualidad, los sistemas de soporte a bordo, los sistemas GPS y los sistemas de conectividad [89] se han vuelto indispensables en la arquitectura de un vehículo. Con esta tecnología, la conducción autónoma [96] se ha hecho posible, el rastreo satelital de unidades puede realizarse sin ninguna restricción, es posible utilizar sistemas de navegación para llegar a lugares desconocidos, hay disponibilidad de sistemas de emergencia en carreteras y la comunicación entre vehículos con el entorno y las unidades RSU (Roadside Unit) permiten muchas más funciones.

No obstante, a medida que los vehículos se vuelven más sofisticados, los casos de robo de vehículos se vuelven más comunes e incluso podrían no disminuir en los próximos años. Aunado a esto, los datos generados en la red interna del vehículo no cuentan con protección. Además de la reciente necesidad de compartir información con el entorno carecen de sistemas de protección de información que impidan obtener, inyectar o manipular datos internos del vehículo [108]. Incluso los ciberataques remotos con teléfonos inteligentes son efectuados sin ninguna complicación.

Debido a estos problemas, en este trabajo se plantea desarrollar un método enfocado en él cifrado de datos del vehículo para el Internet de los vehículos. Se implementará y analizará un sistema de cifrado híbrido basado en los esquemas de cifrado simétrico y asimétrico. El objetivo es garantizar la confidencialidad, la integridad y la disponibilidad de los datos en ambientes públicos IoV. La idea es generar herramientas que permitan un intercambio seguro de información entre el vehículo con su entorno, en el que se agregan aplicaciones como la comunicación [94] V2I (Vehículos a Infraestructura)(como el estado del semáforo, los señalamientos de circulación en carretera), V2E (Vehículo a Entorno)(como la presencia de peatones, aplicaciones de rastreo vehicular), V2V (Vehículo a Vehículo) (como la proximidad con otros vehículos, la ubicación geográfica, etc) y V2P (Vehículo a Peatón) (como las aplicaciones móviles, advertencias de cercanía, detección de personas).

Capítulo 1

1.1. **Introducción**

El crecimiento acelerado de las ciudades y el aumento de la población a nivel mundial ha generado varios desafíos que deben ser resueltos para que la forma de vida sea adecuada. En la actualidad, las ciudades modernas [126] se caracterizan por ofrecer muchos servicios de confort, vanguardia y estilo de vida adecuado para la población. Son muchos los factores implicados para lograr lo antes mencionado como una infraestructura adecuada, desarrollo de tecnología de vanguardia, implementación de sistemas de comunicación, uso de sistemas de transporte eficientes, entre otras.

Muchas de las soluciones planteadas toman en cuenta el uso de la tecnología como herramienta principal (robótica, conectividad, internet de las cosas, inteligencia artificial, ciberseguridad, etc). Gracias a estas tecnologías se pueden realizar un sinfín de proyectos, aplicaciones o programas cuyo principal objetivo es modernizar una ciudad, eficientar servicios, reducir niveles de contaminación y agilizar la forma de vida de la población. En este sentido, conceptos como las ciudades inteligentes y el internet de las cosas han tomado una gran fuerza [126]. Estas tecnologías suelen utilizarse con el simple propósito de monitorear muchos procesos que tienen que ver con los hogares inteligentes como la domótica, el desplazamiento de unidades móviles en el internet de los vehículos [57], la vigilancia aérea en el internet de los drones [28], entre otros.

En la actualidad, para que el estilo de vida y el desarrollo de actividades diarias se mantengan, los medios de transportes son muy importantes. El simple hecho de querer llegar a nuestro destino requiere del uso de un medio de transporte que sea adecuado. Sin contar la gran importancia que han tomado últimamente los medios de transporte para el traslado de bienes materiales, esto solo se ha impulsado cada día más gracias a los servicios de compra y venta en línea y los servicios de mensajería.

No es de extrañarse que debido a la gran cantidad de mercancía, productos e incluso de personas que se trasladan de un lugar a otro, existan accidentes o casos de robo durante el traslado. Estos suponen una gran pérdida monetaria para los consumidores como para las empresas. Derivado de esta problemática, los sistemas GPS fueron implementados como una contramedida para monitorear constantemente varias unidades que trasladan bienes materiales, lo cual, permitió gestionar de forma eficiente flotillas de transporte y promover mejores rutas y mejores costos de traslado, etc [8,9]. Con estos servicios es posible conocer la información precisa de dónde, cuándo, quién y cómo se encuentran algunas unidades así como el conductor.

Gracias al uso de las computadoras en los vehículos, nuevas tecnologías fueron implementadas, de este modo, se marcó una nueva era en la industria automotriz. Dichas tecnologías lograron ofrecer un mejor funcionamiento de los sistemas con mayores prestaciones, mejores tiempos de reacción y respuesta, más rápidos y más precisos [82]. Una desventaja significativa fue que los datos no se encuentran protegidos contra personas ajenas (hackers) que quieran obtener algún beneficio, que en ocasiones pueda perjudicar el correcto funcionamiento de la unidad o atentar contra los pasajeros. De hecho se ha demostrado que la información de los vehículos son susceptibles a ser manipulados y por lo tanto realizar alguna actividad ilícita [109].

Derivado a esta problemática, es importante implementar métodos capaces de salvaguardar la privacidad de la información generada tanto en los vehículos como en los entornos IoV (del inglés Internet of Vehicles). Se plantea analizar herramientas de seguridad como los sistemas blockchain, algoritmos de cifrado de datos y sistemas que sean capaces de obtener, procesar e intercambiar información del vehículo para que el proceso de comunicación sea más seguro. El objetivo que se persigue es que algún agente externo o atacante sea incapaz de adquirir o en su defecto comprender el contenido de la información que ha adquirido durante algún ciberataque.

1.2. Planteamiento del problema

El estilo de vida que tienen las sociedades humanas al día de hoy se ve influenciado por el desarrollo y consumo de nuevas tecnologías. Los servicios e infraestructura se han desarrollado cada vez más para satisfacer las necesidades de la población.

Para las ciudades inteligentes [126] el Internet de las cosas como el Internet de los vehículos se ha vuelto una herramienta muy importante ya que estas permiten automatizar y monitorear muchos procesos o actividades de la vida diaria en una sociedad, como el flujo vehicular, niveles de contaminación, calidad de aire, flujo de personas, gestión de comercios, etc. En el caso específico de un entorno del internet de los vehículos podemos observar una constante evolución. Muchas empresas automotrices comienzan a implementar esta tecnología en sus nuevos modelos. Incluso, el mercado vehicular ha incrementado [INEGI parque vehicular 2022] estos últimos años debido a la alta demanda de movilidad de personas como de productos . Esto solo aumenta el número de unidades que son conectados a Internet sin tomar en cuenta que poco a poco se añaden nuevas unidades que con tecnologías de conducción autónoma.

Gracias a las nuevas tecnologías incorporadas en los vehículos, los servicios ofrecidos son cada vez más eficientes y amigables con los usuarios. Algunas cuestiones de seguridad contra robo de unidades provoca que muchos fabricantes opten por implementar sistemas de rastreo satelital, sistemas de video vigilancia y sistemas de conexión a bordo. Esto último permitió el desarrollo de nuevas aplicaciones [94] como la comunicación del vehículo con el entorno , los servicios de navegación y los servicios de rastreo.

Una de las problemáticas encontradas fue la falta de protocolos de seguridad en la red interna de los vehículos y en la arquitectura de los entornos IoV. Para el caso de los vehículos, las computadoras que gestionan e intercambian información sobre los diferentes sistemas (motor, dirección, transmisión, etc) están expuestas a agentes externos. En la gran mayoría de los casos, es posible acceder a la red interna a través del puerto OBD que da acceso al CAN bus (del inglés Control Area Network) [87,88] donde circula la información.

En el caso de un entorno IoV, el panorama es similar, es decir, la información intercambiada no se encuentra protegida contra agentes externos. Para comprender de mejor manera, debemos tomar en cuenta que una arquitectura IoV consta de 3 elementos principales: los vehículos, los servicios de almacenamiento en la nube y las aplicaciones que puedan ser utilizados por los usuarios u otros dispositivos. En esta arquitectura, los vehículos recopilan información de forma constante y la almacenan en la nube para que las diferentes aplicaciones tengan acceso a los datos. De esta manera, el usuario podrá visualizar de manera gráfica los datos recopilados en alguna aplicación (móvil, web, scripts internos, etc) como la localización del vehículo, la disponibilidad de combustible, etc. Para el caso de los vehículos inteligente y autónomos, dicha información le permitirá tomar decisiones como evadir obstáculos, localizar paso de peatones, seleccionar alguna ruta de circulación, identificar sitios de congestionamiento, etc.

El principal problema radica en que el intercambio de información entre los diferentes elementos se realiza sin contar con medidas de seguridad [17-19] que protejan los datos intercambiados contra hackers. En algunos casos, estas personas podrían realizar algún ataque de ciberseguridad para acceder y obtener diferentes datos. Existen muchos ejemplos de ataques que pueden ser realizados, como acelerar el vehículo, abrir la puerta del automóvil, drenar la batería o la gasolina, obtener los datos de ubicación del carro e incluso engañar al sistema enviando coordenadas falsas para que el vehículo acuda a dicha localización.

En la actualidad existen diferentes métodos que permiten obtener e inyectar información en la red de comunicación de un vehículo. Estos métodos van desde la conexión física al puerto OBD del vehículo, hasta la conexión remota con la ayuda de un teléfono inteligente.

Como se ha visto, pese al desarrollo de medidas de seguridad para salvaguardar la integridad física de los vehículos como la de los usuarios; los datos generados por los diferentes dispositivos y los vehículos en ambientes IoV pueden ser vulnerados por la falta de protocolos que protejan la red de comunicación.

Por tal motivo, es importante que se implementen herramientas de ciberseguridad para proteger los datos generados en un automóvil, especialmente si existe una tendencia a implementar sistemas que requieran conectividad a la red.

1.3. **Justificación**

La implementación de nuevas tecnologías en la industria automotriz, la carencia de sistemas de ciberseguridad [20,21] para la protección de datos internos del vehículo y la falta de protocolos de seguridad en los puntos de acceso a la red vehicular, hacen que estos sean susceptibles a recibir ataques. Estas vulnerabilidades pueden alterar el correcto funcionamiento del vehículo (dejar inoperativo el automóvil, desactivar los frenos, desactivar el sistema de monitoreo GPS, etc). Incluso existen antecedentes y evidencia donde se puede atentar contra la seguridad de los usuarios como ocasionar lesiones al provocar algún choque, obtener datos de localización o personales, acelerar el vehículo para lesionar transeúntes, etc [22].

En el caso de las tecnologías de conectividad (permite la comunicación del vehículo con el entorno) implementadas en los vehículos el panorama no cambia mucho. La transferencia de datos carece de procedimientos de seguridad contra robo e inyección de datos. De hecho, acceder y manipular información de forma remota se vuelve cada vez más fácil [17]. En general, estas brechas de seguridad son muy peligrosas para el correcto funcionamiento del automóvil y la seguridad del consumidor.

Derivado de esta problemática es necesario implementar sistemas de seguridad que tomen en cuenta los datos generados en el vehículo para garantizar la confidencialidad e integridad de los datos. Estas son algunas de las características que se quieren alcanzar en los servicios de emergencia, de seguridad y de financiamiento, es decir, buscan que los datos recopilados sean confidenciales e íntegros. De esta manera se puede evitar que el vehículo sea rastreado de manera ilegal y sin el consentimiento del propietario, y que el intercambio de información de un vehículo a otro o con las unidades RSU (del inglés Roadside Unit) sea seguro.

De esta manera, utilizar sistemas de cifrado de datos puede ser una herramienta útil que permita dar protección a la información intercambiada en los sistemas IoV. El objetivo es que los datos sean incomprensibles por agentes externos cuando se realice algún ataque de ciberseguridad. Incluso los sistemas de cifrado más complejos como el cifrado híbrido puede ser implementado de forma correcta en dichos ambientes.

1.4. **Objetivos**

1.4.1. **Objetivo General**

Implementar un marco de trabajo en el contexto del Internet de los vehículos que considere el intercambio de datos del automóvil como el estado del vehículo, la ubicación geografica y datos sobre el entorno así como el cifrado de mensajes entre los diferentes elementos involucrados asegurando la confidencialidad y seguridad de los datos.

1.4.2. **Objetivos Específicos**

- Estudiar y analizar trabajos relacionados con el proyecto.
- Estudiar y analizar los datos que proporcionan las computadoras de los vehículos actuales.
- Diseñar un procedimiento para la extracción de datos de la computadora del vehículo incluidos los datos GPS y el entorno.
- Diseñar un sistema de cifrado para asegurar los datos obtenidos del vehículo en un ambiente del Internet de los vehículos.
- Implementar el marco de trabajo propuesto en un caso de estudio real.

1.5. **Hipótesis**

Es posible implementar un sistema de seguridad basado en algoritmos de cifrado híbrido que sea capaz de salvaguardar la información compartida por los vehículos en ambientes IoV entre los que se incluyen los datos internos del vehículo, datos GPS y datos del entorno para evitar que un agente externo pueda comprender la información.

Capítulo 2. Estado del arte

En la actualidad, cada segundo circulan una gran cantidad de vehículos por las carreteras. Muchos de ellos se encargan de transportar personas, materias primas, bienes materiales, vehículos, entre otros.

Debido a las condiciones actuales de la sociedad con respecto a la seguridad vial. Existe la posibilidad de sufrir accidentes o asaltos que terminen en grandes pérdidas monetarias. Por lo tanto, gracias al desarrollo de las tecnologías como el Internet de las cosas, muchas industrias han optado por desarrollar e implementar algún sistema basado en esta tecnología para el rastreo satelital de unidades vehiculares.

Los sistemas basados en entornos de Internet de las cosas que son óptimos para la industria automotriz han dado lugar a lo que se conoce como “internet de los vehículos”.

Como se ha comentado, este tipo de tecnologías ha permitido que muchos usuarios sean capaces de monitorear la ubicación exacta de alguna unidad. Su uso ha aumentado considerablemente en las grandes industrias automotrices o de traslado de bienes materiales.

A continuación se describen algunos trabajos relacionados con la implementación de sistemas de Internet de los vehículos. En primera instancia se introducirán algunos sistemas de rastreo que son comercializados hoy en día. Posteriormente se hablará sobre algunos de los trabajos que implementan sistemas de rastreo vehicular. No obstante, estos sistemas carecen de protocolos de seguridad contra hackers, por lo que en el siguiente punto se abordarán algunos trabajos que marcan la importancia de los sistemas de ciberseguridad para evitar el robo y manipulación de datos en los entornos IoV. Derivado de esto, los siguientes apartados se presentarán una serie de trabajos que emplean sistemas de rastreo vehicular aplicando algún protocolo de seguridad para la protección de los datos GPS como IoV.

2.1. **Sistemas de rastreo vehicular**

En el mercado existen algunos productos que ofrecen servicios de localización en tiempo real, independientemente de la ubicación y las condiciones en las que se encuentre. En la Tabla 1, podemos observar algunos de los sistemas de rastreo vehicular que son comercializados hoy en día. Además, se describen algunas de sus características principales y qué servicios ofrecen al consumidor.

Onstar. Subsidiaria de General Motors que brinda servicios de seguridad a bordo de vehículos, servicios de emergencia, sistemas de diagnóstico remoto y sistemas de localización. Este es un servicio de pago mensual que va desde los $250 hasta los $600.

Lo/Jack. Ofrece servicios de rastreo, monitoreo y recuperación de unidades con visibilidad e información en tiempo real. Ofrecen asistencia durante la conducción y de recuperación en caso de robo. Este servicio es de pago mensual.

Samsara()GPS tracker). Ofrece servicios de localización del vehículo en tiempo real. Da acceso a información sobre el estado del vehículo. Además ofrece asistencia durante la conducción.

FOAM Location. Proporciona servicios de localización mediante GPS con apoyo de hardware LPWAN. Sus servicios son de pago y se realizan mediante depósitos de tokens.

Como se observó en la Tabla 1, la cantidad de servicios de rastreo vehicular no es muy extensa y en ocasiones puede ser algo cara. Derivado de la falta de más sistemas o productos que se encarguen de ofrecer servicios similares se abordan diferentes propuestas que se han desarrollado con este enfoque. Actualmente muchos de estos trabajos se han implementado tomando en cuenta algún tipo de servicio adicional.

Por ejemplo, Dongdong Yuan et al. [5] diseñan un modelo matemático enfocado en el seguimiento de la trayectoria de vehículos no tripulados. Su modelo está basado en un método de control adaptativo. Además realizaron una serie de simulaciones matemáticas que muestran que su algoritmo adaptativo para la localización de vehículos no tripulados es efectivo.

En su artículo, Xiangdi Liu et al. [6] proponen un marco de seguimiento multicámara de vehículos en carreteras en tiempo real. Resaltan la importancia del uso de cámaras de video vigilancia en carreteras para la vigilancia inteligente. Su propuesta contempla un sistema basado en aprendizaje profundo llamado VTC (Vehicle Tracking Context) para extraer características del contexto. Dicho sistema está dividido en dos etapas, la detección y la reidentificación de vehículos. La identificación de vehículos se centra en la caracterización de la apariencia o textura de un vehículo. Sus resultados experimentales que fueron probados físicamente en carretera, demuestran una alta eficacia.

Por su parte, Taku Noguchi et al. [7] proponen un método de rastreo de vehículos mediante el uso de VANETs. Su método contempla la participación y cooperación de vehículos y unidades de carretera (RSU) para obtener la ubicación de algún objetivo. El seguimiento ininterrumpido de un vehículo lo logran a través de un rastreador que transmite una solicitud a los vehículos circundantes para no perder el objetivo. Sus experimentos involucran el uso de un simulador de red para evaluar la efectividad y desempeño de su propuesta. Los resultados obtenidos demuestran que dicho método es capaz de lograr el seguimiento en tiempo real e ininterrumpido de unidades objetivo.

Asep Najmurrokhman et al. [8] proponen un prototipo de registro de velocidad del vehículo que utiliza un rastreador GPS y una plataforma de Internet de las cosas (IoT). Su enfoque está orientado a observar la velocidad del vehículo, para que el conductor no exceda el límite máximo de velocidad en la carretera. Para ello, utilizan un GPS que determina la ubicación del vehículo y calcula la velocidad del automóvil mediante un módulo SIM808 y un microcontrolador Arduino. La ubicación y la velocidad del vehículo son almacenados en un servidor web dedicado, y los datos son mostrados en una plataforma IoT llamada Adafruit IO. Los resultados muestran que el prototipo puede mostrar la ubicación con alta precisión. Sin embargo, observaron que existe una discrepancia de velocidad promedio de 3,9 km/h durante un viaje.

Por otro lado, Ning Li et al. [9] proponen un método de detección y seguimiento de objetivos utilizando la teoría de fusión multisensor. Su método es capaz de lograr una detección y un seguimiento estable de vehículos tanto estáticos como dinámicos. Como herramientas utilizan tecnologías de escaneo 3D-Lidar, sistemas de detección radar de ondas milimétricas y sistemas de rastreo GPS/IMU. La forma en que funciona su modelo contempla el usos de los sistemas 3D-Lidar para detectar el modelo geométrico del vehículo e iniciar su seguimiento. Luego, el objetivo dinámico (en movimiento) es rastreado a través de un radar de onda milimétrica. Finalmente utilizan los dispositivos GPS/IMU para obtener información sobre su posición relativa. Los experimentos realizados involucraron entornos no estructurados (como tramos accidentados, abruptos e irregulares). Observaron que la velocidad máxima de seguimiento en este tipo de terrenos es de 40 km/h con máximas distancias de hasta 100 metros. De esta manera demuestran que su modelo es adecuado para la detección y seguimiento de vehículos en entornos no estructurados.

Sumalatha Aradhya et al. [10] proponen un método para rastrear algún vehículo y notificarlo. Ellos implementan un algoritmo que transmite datos desde el vehículo rastreado. También implementan una aplicación móvil que les permite rastrear y verificar la velocidad del vehículo. En sus experimentos, utilizan un sensor RFID y una pantalla frontal para rastrear y analizar la velocidad o ubicación del vehículo en todo momento. Dan especial enfoque a dar solución a problemas de posibles robos donde los datos recopilados sobre el vehículo serán compartidos con el conductor y las autoridades correspondientes.

Kai Tian et al. [11] proponen un módulo de seguimiento basado en sistema de vista aérea o BEV (por sus siglas en inglés de Bird´s eye View) y un método de correlación de objetivos para tareas de seguimiento. Discuten que los datos de tráfico en los entornos BEV contienen información sobre el objetivo así como datos dimensionales. Sus resultados demostraron que con la proyección de objetos en 3D mediante el método BEV se puede lograr una mejora significativa en las tareas de detección, seguimiento de trayectoria, planificación de rutas, etc.

Ciyun Lin et al. [12] proponen un método de detección y seguimiento de vehículos basado en tecnología LiDAR de canal bajo para entornos complejos. Estipulan que el seguimiento completo de los objetivos dentro de un rango específico de escaneo es una tarea algo difícil, en especial en situaciones de tráfico pesado. Dentro de su modelos utilizan el método de ajuste en L para obtener un cuadro delimitador más preciso donde se puedan extraer características más precisas del objetivo. Luego, utilizan un árbol de decisiones para clasificar objetos de tráfico. Posteriormente, utilizan un algoritmo húngaro mejorado junto con el filtro de Kalman para predecir la trayectoria del vehículo. Finalmente, miden la efectividad del modelo propuesto al comparar los datos LiDAR recopilados durante la conducción por carretera con los datos obtenidos de diferentes cámaras de vídeo. Los datos de video son obtenidos con un software llamado VeloView el cual permite visualizar nubes de puntos. Sus resultados muestran que la precisión de detección y seguimiento de su modelo alcanza el 99.50% y el 97% respectivamente.

Zhanbo Sun et al. [13] proponen un marco de seguimiento de vehículos por lotes utilizando teoría de fusión de datos, integración de información (DFII-VT) y programación dinámica (algoritmo de Kuhn-Munkres). Su propuesta puede formularse como un modelo

de optimización combinatoria. Para comprender de mejor manera su modelo, los datos de tráfico, las decisiones durante cambio de carril, los tiempos de viaje, las características del vehículo y los datos históricos se integran en el modelo para obtener resultados más precisos. De este modo, se obtienen mejoras significativas en la precisión a medida que se integra más información en el modelo. Los resultados experimentales muestran que la fusión de datos en problemas de detección y ubicación de automóviles produce mejores resultados comparado con los modelos que usan información de una sola fuente.

Bo Yang y colaboradores [14] presentan un método de seguimiento de vehículos en escenarios de tráfico y se apoyan de un marco de seguimiento basado en la detección (DBT del inglés Detection-Based Tracking). Para diseñar el modelo de detección de vehículos se utiliza el modelo YOLO (del inglés You Only Look Once) y luego combinan la información de los atributos del objetivo con los datos de la intersección sobre unión (IOU del inglés Intersection Over Union). Los valores de observación y de predicción son combinados y procesados para lograr un seguimiento más estable. Además utilizan información como la posición espacial, la dirección del movimiento y los datos históricos del objetivo para lograr un seguimiento continuo. Esto permitirá modificar y mejorar el cuadro de detección de los vehículos lo que también mejora la precisión.

Xiaoxu Liu et al. [15] presentan un método para detectar y rastrear vehículos en el contexto de la conducción autónoma y escenarios relacionados con fallas del vehículo. Estipulan que deben garantizar la identificación y el seguimiento precisos de los vehículos para mejorar la seguridad vial. Su método está basado en algoritmos de aprendizaje profundo mediante una red siamesa híbrida que fusiona las capacidades de los modelos YOLO con los Transformers. Esta integración tiene como objetivo facilitar la detección y el seguimiento preciso de múltiples vehículos.

La Tabla 2 muestra un resumen general de los trabajos relacionados con los sistemas de rastreo vehicular que se han desarrollado.

2.2. **Brechas de seguridad en los vehículos**

Al observar los servicios y trabajos anteriores podemos observar que fueron desarrollados sin tomar en cuenta temas de ciberseguridad. Hoy en día esto es una gran brecha de seguridad dentro del sistema de un vehículo, por tal motivo es importante acatar e implementar metodologías de ciberseguridad que proporcionen seguridad a los datos. En la literatura son innumerables la cantidad de trabajos relacionados con la ciberseguridad en los vehículos para mitigar en lo más posible las brechas de seguridad.

Entre estos trabajos podemos encontrar aquellos trabajos que intentan dar a conocer y demostrar que los vehículos poseen una gran cantidad de brechas de seguridad, y por lo tanto, son susceptibles a recibir una gran variedad de ataques. También se encuentran aquellos que proponen alguna herramienta que sea capaz de evitar o en su caso mitigar en lo más posible los ataques realizados.

Para comenzar, Shumei Liu et al. [16] proponen un método de análisis de vulnerabilidad para identificar de manera efectiva vulnerabilidades en áreas críticas de los entornos IoV. Su análisis está enfocado principalmente en la conectividad dinámica y en la integridad de las áreas críticas. Discuten que la heterogeneidad de los servicios IoV y los fallos que pudieran existir, dañen seriamente la conectividad y el rendimiento del sistema. En la actualidad existe una carencia de métodos fiables para analizar vulnerabilidades en la conectividad y además muchos de estos ignoran la existencia de áreas críticas dentro del sistema. Derivado de esto, utilizan un método de partición espectral para identificar elementos que puedan dañar gravemente la conectividad del sistema y perjudicar áreas críticas. Los resultados de sus experimentos muestran que su método puede identificar eficazmente elementos vulnerables para evitar pérdidas en el rendimiento de los sistemas IoV.

En su investigación, Yousik Lee et al. [17] presentan un método de análisis de ciberataques basado en cadenas de destrucción cibernética para crear un sistema que sea capaz de identificar vulnerabilidades. Estipulan que la tendencia emergentes en la industria automotriz deriva en nuevas tecnologías de electrificación, de conducción autónoma, de uso compartido y de conectividad lo que aumenta la cantidad de vulnerabilidades. Por tal motivo, realizan un estudio sobre trabajos previos de hackeo de vehículos reales para identificar algunas características de ataques o las técnicas que son utilizadas en el hackeo de vehículos. Su objetivo es proponer algunas medidas de defensa ante algún ataque. Derivado de esto, proponen un sistema que pueda exponer vulnerabilidades comunes en el automóvil, Su sistema se encargará de gestionar y compartir información sobre los ciberataques, amenazas y vulnerabilidades en los vehículos.

Ahmed Abdullahi et al. [18] proponen un método genérico para evaluar vulnerabilidades en los sistemas de comunicación de red para los entornos IoV. Su caso de estudio está enfocado en realizar un ataque de falsificación de datos GPS en vehículos conectados. En sus experimentos utilizan un UGV (vehículo terrestre no tripulado) como caso de estudio. Además realizan un estudio que tiene como objetivo enfatizar la importancia que tiene la ciberseguridad al diseñar nuevas tecnologías, implementar medidas de seguridad mínimas y el valor que tienen las medidas de control de acceso para reducir amenazas en los sistemas Wi-Fi que son utilizados en las comunicaciones V2X. Sus resultados experimentales demuestran la existencia de vulnerabilidades que permiten tomar el control total y manipular la navegación de los UGV.

Manuel Mar et al. [19] realizaron un estudio de análisis de vulnerabilidades y amenazas en un vehículo eléctrico. Su enfoque está dirigido a analizar los sistemas de comunicación con el fin de recopilar mensajes del bus CAN sobre las ECU (Unidad de Control Electrónico o en inglés Electronic Control Unit) y el BMS (Módulo de Gestión de Batería). Tiene como objetivo inyectar mensajes falsos para analizar el comportamiento de los vehículos eléctricos. En sus resultados descubrieron que debido a la diferencia de comunicación entre el motor y las ECU, el rendimiento energético se vio comprometido. Incluso, observaron que el sistema de propulsión de un coche eléctrico puede degradarse gravemente cuando no se activan los sistemas de advertencia de avería.

Yinghui Wang et al. [20] proponen un método de evaluación de vulnerabilidad para las tecnologías CAV (Vehículos Conectados y Autónomos). Adoptan el sistema de puntuación de vulnerabilidad (CVSS) y la teoría de Bayes para escalar la gravedad de

vulnerabilidad del sistema. Discuten que a medida que se incorporan más tecnologías en los vehículos, las tecnologías CAV se vuelven más vulnerables. Por tal motivo se debe dar máxima prioridad a aquellas vulnerabilidades que puedan poner en peligro la vida de los usuarios. En sus experimentos utilizaron diferentes conjuntos de datos y algoritmos, los resultados indican que el modelo es capaz de evaluar la vulnerabilidad de los vehículos de manera eficaz.

Shen S. Shiwen et al. [21] realizan una investigación que está centrada en la identificación de métodos para detectar vulnerabilidades en vehículos inteligentes conectados. Para ello utilizan componentes inteligentes de los vehículos conectados, definen diferentes vectores de ataque, adoptan sistemas CWE (Enumeración de Debilidades Comunes), utilizan tecnología de escaneo de vulnerabilidades para el firmware de los vehículos conectados y hacen uso de un marco de procesamiento de datos con el fin de llevar a cabo un análisis de vulnerabilidades. Sus hallazgos demuestran la importancia de mejorar la seguridad de los vehículos conectados.

En su investigación Yujia Li et al. [22] identificaron riesgos de seguridad potenciales para los datos en el ámbito de los vehículos inteligentes e IoV. Su enfoque está dirigido hacia los sistemas de procesamiento de datos de vehículos inteligentes y conectados para mitigar los riesgos de seguridad que pueden conllevar riesgos demasiados altos. Sus experimentos los realizaron mediante el análisis de paquetes de datos. Los resultados obtenidos indican que existen una gran cantidad de riesgos de seguridad que involucran datos personales, datos de ubicación y datos biométricos.

Yuvraj Singh et al. [23] realizaron un estudio sobre los ataques basados en cadenas de muerte cibernética (cyber-kill-chain) para crear un sistema de análisis de vulnerabilidades que permita optimizar la seguridad en los vehículos. Su enfoque va dirigido al análisis de vulnerabilidades en los vehículos de versión eléctrica, con instalaciones de inteligencia artificial, con sistemas de seguimiento del tráfico, sistemas G.P.S. y autónomos. Su objetivo es encontrar puntos clave en el momento de un ataque y proveer de un mecanismo automatizado que detecte, exponga alguna vulnerabilidad y proponga alguna medida de seguridad.

Zaina Abuabed y compañía [24] proponen un marco de análisis de ciberseguridad que está basado en la norma de seguridad ISO/SAE 21434:2021. Este marco utiliza modelos de amenaza de suplantación de identidad, manipulación, repudio, divulgación de información, denegación de servicio, elevación de privilegios (STRIDE), el enfoque de análisis de árbol de ataques (ATA). Utilizan como sistema de puntuación al CVSS (Sistema de Puntuación de Vulnerabilidad Común) para calificar las amenazas que fueron identificadas. Para evaluar su modelo, utilizaron escenarios de la vida real donde evaluaron a los sistemas avanzados de asistencia al conductor (ADAS). Como resultado, se identificaron 199 amenazas relacionadas con estos sistemas. Esto demuestra que la tecnología ADAS en los vehículos modernos son vulnerables a los ciberataques.

Huimin Chen et al. [25] realizaron una investigación exhaustiva sobre los problemas de seguridad (vulnerabilidades, ataques y contramedidas) que existe en la red de comunicación interna de un vehículo. Por lo tanto, existe una necesidad urgente de proponer soluciones novedosas y ligeras (debido a los recursos limitados de las computadoras automotrices) para dar seguridad a las comunicaciones del vehículo. Además, analizan algunos sistemas de normalización que están relacionados con los problemas de seguridad en la comunicación interna del vehículo. Por último, discuten y presentan algunas soluciones que permitan proteger la red de comunicación dentro del vehículo para mejorar la seguridad.

En su trabajo, Gianpiero Costantino e Ilaria Matteucci [26] recalcan que el sistema de comunicación interno de un automóvil posee accesos de entrada que permitan ejecutar ataques de ciberseguridad. La red fue diseñada desde un principio con problemas de seguridad, ya que los mensajes que se intercambian en la red del vehículo vía CAN, se hace en un formato de texto en claro. Por tal motivo el acceso no controlado al CAN bus puede tener graves repercusiones que se verán reflejadas en problemas de integridad del sistema como en la seguridad de los usuarios. Incluso, este problema solo se ve engrandecido gracias a los sistemas que permiten conectar al vehículo con una red wifi. En su trabajo, presentan un sistema de evaluación de vulnerabilidad mediante un proceso de ingeniería inversa. Como caso de estudio, analizan las vulnerabilidades de un vehículo Kia donde pretenden comprometer su funcionalidad al inyectar tramas CAN o alterar el comportamiento del vehículo. Como resultado lograron identificar cuatro tipo de vulnerabilidades importantes que afectan a los vehículos Kia.

Amala et al. [27] proponen un sistema enfocado en la extracción y análisis de rastros digitales en los sistemas de seguimiento de vehículos. Pretenden utilizar técnicas de análisis forense para encontrar y extraer pruebas claras relacionados con incidentes vehiculares. En su trabajo incluyen la extracción de datos forenses y el análisis de artefactos del ecosistema IoV. Además, hacen uso de una herramienta de prueba IoT Forensics Suite (IFS) que fue desarrollada durante la investigación. Incluso la herramienta que desarrollaron muestra gran viabilidad para realizar análisis forenses en otros dominios de IoT.

La Tabla 3 muestra un resumen y comparación entre los trabajos que tienen relación con estudios de ciberseguridad (brechas de seguridad y vulnerabilidades) en los automóviles.

2.3. **Cifrado de datos GPS para ambientes IoV**

Actualmente, muchas tecnologías de Internet de los vehículos utilizan dispositivos satelitales vía GPS. El uso del GPS en los vehículos ha aumentado gradualmente, en especial para los sistemas de rastreo así como en los vehículos autónomos. Sin embargo, se ha demostrado que los datos GPS pueden ser obtenidos y manipulados. En consecuencia, se han propuesto diferentes proyectos relacionados con el cifrado de datos GPS para tener un mejor nivel de seguridad.

Por ejemplo, Shenqing Wang et al. [28] proponen un método de detección de ataques para tecnologías de vehículos aéreos no tripulados (UAV). El GPS desempeña una tarea muy importante en las funciones de navegación de las UAV. Sin embargo, la comunicación se encuentra abierta y es por lo tanto es inseguro el ambiente. Los hackers pueden obtener señales GPS reales para lanzar ataques de suplantación GPS. Como contramedida, utilizan un algoritmo de aprendizaje automático llamado LSTM (del

inglés Long short-term memory) o memoria a corto plazo para detectar ataques de suplantación de identidad de datos GPS. En su trabajo detallan el funcionamiento del algoritmo encargado de percibir ataques de suplantación de GPS. Los experimentos se realizan en un entorno de simulación. Afortunadamente, logran detectar de manera satisfactoria, rápida y precisa ataques de suplantación de información GPS.

Shenzheng Zuo et al. [29] también proponen un método de detección de ataques de suplantación GPS. Su método está basado en los algoritmos de bosque de aislamiento. En su propuesta utilizan imágenes satelitales como fuente de datos. En ellas analizan cada dato para evaluar si los datos son normales o anormales y así determinar si existe algún ataque de suplantación de identidad GPS. En las simulaciones, comparan diferentes muestras con características satelitales variadas. Los resultados alcanzan un 95 % de precisión al analizar diferentes muestras. Como resultado demuestran que los sistemas que utilizan datos GPS pueden ser manipulados fácilmente para realizar algunos ataques.

Por otra parte, Ibraheem y Hadi [30] proponen un modelo que se apoye de la tecnología inalámbrica XBee debido a los privilegios que brindan en términos de bajo costo y un alto nivel de seguridad. Además brindan una transferencia de información más confiable, evita la penetración de datos y el acceso no autorizado sin ningún costo. Para el envío y recepción de información, el sistema en general consta de 2 módulos principales: el módulo de visualización (estación de control) y el módulo de seguimiento (unidad del vehículo). El módulo de seguimiento consta de una plataforma Arduino, un XBee y un módulo de navegación GPS. El módulo GPS entrega datos en tiempo real sobre la ubicación del vehículo y dirige las coordenadas al XBee a través de la plataforma Arduino. Recibir los datos de ubicación del vehículo rastreado y mostrarlos de forma segura en Google Earth es responsabilidad de la estación de monitoreo. El sistema diseñado ha sido probado prácticamente en entornos concurridos y en áreas abiertas. El sistema en general funciona bien y muestra de forma segura las coordenadas del vehículo.

En este caso, Gupta et al. [31] desarrollaron un método que aplica cifrado homomórfico para proporcionar privacidad a los datos de ubicación. Esto se hace en compañía del sistema de posicionamiento global GPS para calcular las coordenadas geográficas de la ubicación del usuario. El cifrado homomórfico es un proceso a través del cual el texto sin formato se convierte en texto cifrado. Con este cifrado se puede trabajar para que el texto cifrado o modificado estuviera en su forma de texto sin formato. Para ello utiliza operaciones matemáticas en los datos cifrados sin comprometer el cifrado ni tener que descifrar. El principal problema con el cifrado homomórfico es que es muy lento, sin embargo es posible mejorarlo si se mejora la velocidad y se aumentan los cálculos de suma y de multiplicación necesarios.

Daven Darmawan Sendjaya et al. [32] desarrollan un dispositivo de detección de distancia incorporando sistemas de cifrado para la transmisión segura de datos a través del protocolo MQTT. El dispositivo incorpora módulos ESP32, GPS y un algoritmo de cifrado llamado “XTEA”. En su propuesta, los datos de ubicación obtenidos con el GPS se cifran antes de enviarse al servidor MQTT. Posteriormente, un segundo dispositivo ESP32 accede a la base de datos MQTT para obtener y descifrar la información. El sistema necesita aproximadamente 25.3µs para cifrar y 34µs para descifrar las coordenadas. Los datos de ubicación descifrados son utilizados para calcular la distancia entre los dos dispositivos ESP32 con la fórmula de Haversine. Los resultados demostraron que el sistema puede calcular distancias y proporcionar un nivel adecuado de seguridad barata (computacionalmente hablando) y eficiente.

Ashish Nanda y colaboradores [33] presentan un protocolo de enrutamiento seguro que está orientado a la geolocalización (Secure-GLOR) para redes de malla inalámbricas. Su modelo incorpora un esquema de cifrado para mejorar la seguridad. Buscan mejorar el rendimiento de la red reduciendo el tamaño de los datos, reduciendo la sobrecarga computacional y acelerando los ciclos de cifrado-descifrado. El esquema de seguridad que propusieron logra buenos resultados de desempeño que son equiparables a otros algoritmos.

Christian Vitale et al. [34] incorporan un modelo de ciberseguridad llamado H2020-CARAMEL con el que buscan mejorar la protección de los datos en los sistemas de comunicación de conducción automatizada y los vehículos modernos. En especial, abordan escenario de ataque de suplantación de GPS. La arquitectura CARAMEL incluye infraestructura de conectividad con soporte simultáneo 802.11p y LTE-Uu, una plataforma MEC que permita implementar algoritmos de detección de ataques, una unidad con funciones inteligentes anti ataques y un sistema de clave pública que valide la integridad de las transmisiones en los vehículos.

Xiaodong Zheng et al. [35] proponen un esquema de emparejamiento de bloques cifrados (EGMS del inglés Encrypted Grids Matching Scheme) para proporcionar un servicio de preservación de la privacidad para cada una de las entidades que participan en el proceso de detección múltiple. En el proceso de detección múltiple, la asignación de tareas es una parte importante, sin embargo, durante este proceso la ubicación de los participantes puede estar comprometida. Como contramedida, los autores utilizan un método de cifrado homomórfico donde cada tarea que fue asignada a cada bloque es cifrada. En general, todo el proceso de emparejamiento de tareas se realiza en un entorno cifrado. En su investigación, exploran cuatro escenarios de aplicación para demostrar la seguridad entre los participantes. Los resultados obtenidos son comparados con otros esquemas similares para demostrar la eficacia del esquema propuesto.

2.4. **Ciberseguridad en sistemas IoT e IoV**

Los trabajos anteriores fueron realizados con el propósito de dar a conocer las brechas de seguridad que existen en los vehículos modernos. Para combatir estas brechas de seguridad se pueden utilizar una gran variedad de herramientas de ciberseguridad como los sistemas de detección de intrusos, sistemas de prevención de intrusiones, firewalls, criptografía, entre otros.

Es importante implementar medidas de seguridad para proteger los datos del vehículo derivado de la evolución tecnológica que presentan los vehículos modernos y el auge que ha tenido la tecnología de Internet de las cosas en la industria automotriz.

Actualmente se pueden observar una gran variedad de proyectos que pretenden dar soporte a las nuevas tecnologías basadas en el Internet de las cosas para la industria automotriz. Entre estas tecnologías podemos encontrar la comunicación vehicular ya sea entre vehículos, con la infraestructura o en general con el entorno.

Para el caso de tecnologías de Internet de los vehículos es importante adoptar medidas de seguridad pues los datos involucrados en la comunicación pueden ser muy importantes. Del mismo modo, a como se haría en alguna otras áreas, la importancia de los datos involucrados requiere de medidas de seguridad adecuadas y más estrictas. Por ejemplo, no es lo mismo dar soporte de seguridad a las calificaciones que obtuvieron los alumnos a los datos bancarios de alguna persona. En el segundo caso se requieren de medidas de seguridad más estrictas para proteger información confidencial.

En la literatura se demuestra que se está realizando mucha investigación en el área de Internet de los vehículos para dar soporte de ciberseguridad a estas tecnologías.

Dang et al. [36] proponen un método de cifrado AES que genera llaves dinámicas. El algoritmo AES se implementa con el objetivo de generar una clave dinámica. En su algoritmo apilan 16 bits de datos en una trama y la transmiten en secuencia. En base a esta secuencia, se producirán cambios que solo mejoran la seguridad del sistema durante la transmisión de datos. El método descrito lo usan como una técnica de codificación para garantizar que los datos que son intercambiados sean irreconocibles por terceros. Esto puede ser de gran ayuda para el intercambio de datos que son sensibles, como podría ser el seguimiento del viaje en un vehículo o datos de su propietario.

Feng et al. [37] proponen un nuevo modelo de cifrado para entornos IoV llamado ABEM-POD. Utilizan un método de cifrado genérico basado en Spark y MapReduce que es aplicable a los esquemas ABE con una estructura de acceso al árbol. Además se puede aplicar a los entornos de Internet de los vehículos. Este enfoque puede mejorar significativamente la velocidad de cifrado para abordar requisitos de tiempo de respuesta para el internet de los vehículos.

Yan Cui et al. [38] proponen un marco que combina al cifrado homomórfico (FHE) y al blockchain para cifrar y registrar los rastros de solicitud en la nube. Existe un gran problema a la hora de enviar datos privados de los fabricantes de vehículos y por tal motivo es importante proteger dicha información. En su propuesta, ellos utilizan un algoritmo de cifrado desarrollado por Microsoft Research que es llamado SEAL (del inglés Simple Encrypted Arithmetic Library) y un marco blockchain desarrollado por IBM Hyperledger Fabric. Sus experimentos demuestran que el marco propuesto puede ser utilizado en sistemas de cómputo en la nube.

Wanli Xue et al. [39] proponen un esquema de cifrado ligero basado en sensores compresivos llamado Kryptein. Su enfoque está dirigido a la protección de los entornos IoT. El sistema Kryptein está basado en el cifrado comprimido aleatorio, el cálculo estadístico sobre cifrado y el descifrado preciso de datos sin procesar. Sus experimentos muestran que Kryptein es robusto y es unas 250 veces más rápido que otros sistemas, además su consumo energético es unas 120 veces menor. También será capaz de soportar tareas básicas del aprendizaje automático.

En su trabajo, Jiawei Zhang et al. [40] discuten las problemáticas que existen en el intercambio de datos en los entornos IoV con la nube y la niebla. Incluso estos problemas pueden incurrir en muchos problemas de seguridad incluida la fuga de datos y la violación a la privacidad de la información. Como respuesta a esta problemática, ellos proponen un esquema seguro para el intercambio de información en los sistemas IoV. En su propuesta, utilizan un cifrado basado en atributos de política de texto (CP-ABE) para garantizar la confidencialidad y gestionar el acceso en los ambientes IoV. En sus experimentos encontraron algunos desafíos que tienen que ver con la dinámica de múltiples vehículos. Para afrontar este desafío, utilizan el concepto de revocación de usuario auditable para aplicar de manera exitosa el cifrado CP-ABE, el cual puede adaptarse a grupos de vehículos dinámicos. Los resultados demuestran que su esquema es eficiente y otorga una seguridad aceptable en el intercambio de información en IoV.

Hassan Karim y Danda Rawat [41] establecen que los sistemas emergentes IoV (especialmente en el rastreo de vehículos) aún no se implementan protocolos de protección de datos de los usuarios. En su lugar, ellos presentan un modelo que permite proteger la privacidad de los datos especialmente para los sistemas de transporte de peaje electrónicos. Su objetivo es preservar la privacidad del conductor y aportar en el desarrollo de sistemas seguros que estén encargados de la gestión inteligente de la infraestructura del transporte. Para abordar dicha problemática, desarrollan una herramienta a la que llaman TollsOnly. Está fue diseñada con un sistema de cifrado de datos homomórfico. Además se apega al reglamento general de protección de datos (RGPD) y a la ley de privacidad del consumidor de California.

Baee et al. 2022 [42] proponen un nuevo esquema seguro y eficiente que preserva la privacidad en protocolos de transmisión anónima para vehículos livianos (ALI). Ali proporciona un alto nivel de anonimato al combinar una escama de autenticación de mensaje con cifrado. También argumenta y demuestra que la sobrecarga criptográfica para la comunicación vehículo a vehículo en el esquema Ali es de solo 149 bytes y pueden gestionar la autenticación de aproximadamente 700 mensajes de difusión cada 100 milisegundos. Esto demuestra lo apto que es el esquema ALI en escenarios de mucho tráfico. Para probar la seguridad y eficiencia de su propuesta realizaron diversas pruebas de comportamiento y un análisis de rendimiento extenso.

Por otra parte, Zhuangjun Ma et al. [43] proponen un método que proporciona seguridad a los datos sensibles de los entornos de cómputo en la nube. Su propuesta combina el cifrado basado en atributos con el algoritmo de cifrado RSA (Rivest-Shamir-Adleman). Las ventajas de este método incluyen una comunicación cifrada de forma bidireccional y un control de acceso robusto, esto garantiza que solo los usuarios adecuados puedan acceder a información. Su propuesta muestra alta robustez ante ataques de intermediario (MITM) y ante riesgos de fuga de datos.

Qi Mu et al. [44] diseñan una tarjeta de cifrado FPGA (Field Programmable Gate Array) que permite la virtualización I/O de raíz única (SR-IOV). Su tarjeta es un dispositivo de función física (PF) que puede gestionar cuatro dispositivos virtuales (VF). Su

arquitectura contempla la implementación de algoritmos criptográficos AES, SHA-256 y además cuenta con funciones de administración de claves. Los resultados experimentales muestran que el dispositivo es capaz de trabajar con velocidades de transferencia de datos de 6,91 GB/s (lectura) y 6,32 GB/s (escritura). El sistema cumple con los requisitos de seguridad para mejorar la privacidad y confidencialidad de datos privados.

Zhuoqun Xia et al. [45] proponen un esquema de privacidad vehicular liviano para los ambientes IoV. Esto debido a que dichos entornos carecen de mecanismos de seguridad permitiendo que los dispositivos involucrados en las comunicaciones como las OBUs (Unidades Vehiculares a Bordo, del inglés Vehicular On-Board Units) o las RSU (Unidades de Carretera del inglés Road Side Units) pueden verse comprometidas. Su modelo utiliza algoritmos de cifrado ligeros basados en atributos para mejorar la seguridad interna de la red vehicular. También proponen un método que permite revelar la identidad de las unidades maliciosas sin revelar información sobre los vehículos auténticos. Sus experimentos demuestran un comportamiento eficiente ante amenazas.

Yuhong Li et al. [46] proponen un método de intercambio de información segura en entornos IoV mediante la implementación de algoritmos de cifrado ABE (Attribute-based encryption) y blockchain. Con los sistemas criptográficos ABE se pueden estipular políticas de acceso a los datos. También utilizan blockchain como un discriminador que aumenta la transparencia de todo el sistema. En su propuesta los datos son almacenados en un sistema de archivos distribuido (IPFS) para mejorar la eficiencia del sistema durante el intercambio de datos. Los resultados experimentales muestran que la propuesta puede compartir datos de forma segura en ambientes IoV.

Wei Tong y Huan Xie [47] diseñan un sistema de adquisición, almacenamiento y cifrado de datos del CAN bus de los automóviles para la protección de datos. La forma de acceder al sistema es a través del puerto serial o con una interfaz USB para obtener diferentes parámetros. En su propuesta , utilizan claves DES para cifrar la información. Posteriormente, hacen uso de un protocolo seguro de datos (PDU) para encapsular y proteger las direcciones de origen y destino. De esta manera el intercambio de información se hace de manera segura, incluso, en ambientes IoV. Los resultados demuestran que el sistema puede ser aplicado de manera exitosa, además ahorra mucho espacio de almacenamiento.

Manjari Singh Rathore et al. [48] presentan un método enfocado en brindar seguridad a los sistemas IoV. Su método utiliza un algoritmo eficiente para la transmisión segura de datos (EAST), el cual implementa mecanismos de cifrado y esteganografía. El sistema EAST propuesto es comparado con algoritmos más conocidos como AES (Advanced Encryption Standard), DES (Data Encryption Standard), G-DES (Generalized DES). De esta manera logran obtener información relevante como el tiempo de cifrado y descifrado, la eficiencia, el efecto de avalancha, la relación de señal/ruido PSNR y el tamaño de la portada del archivo. Los resultados experimentales mostraron mejoras en la eficiencia de tiempo de 0.86 ms, un efecto de avalancha de 58.81% y un PSNR de 78.58%.

Pengshou Xie et al. [49] proponen un algoritmo de cifrado basado en sistemas CP-ABE. Un sistema CP-ABE es un algoritmo criptográfico que gestiona el acceso a la nube. Su propuesta es una versión mejorada llamada VM-CP-ABE para entornos IoV. Tiene como característica principal ofrecer un proceso de cifrado fuera de línea (offline) y un descifrado subcontratado. El cifrado fuera de línea utiliza tiempo en la red vehicular para generar texto cifrado, al mismo tiempo ejecuta procesos de intercambio secretos en cada fase. En el proceso de descifrado subcontratado se generan claves de transformación y gestiona las operaciones de emparejamiento complejas donde el rendimiento es débil. Dichas operaciones complejas son transferidas a unidades subcontratadas más poderosas. Los experimentos muestran que el modelos VM-CP-ABE puede generar texto cifrado más pequeño y en consecuencia evitar problemas de eficiencia de espacio. Los resultados muestran una alta eficiencia en entornos que utilizan servicios en la nube.

En su trabajo, Xiantong Huang et al. [50] estipulan que el CAN bus está teniendo un papel cada vez más importante en el desarrollo del Internet de los vehículos (IoV). Derivado de las carencias del protocolo CAN, ellos proponen un sistema ligero basado en el cifrado en bloques llamado “IoVCipher” para proteger la seguridad de la información en IoV. Además, implementan una estructura MISTY extendida para el proceso de cifrado y descifrado. Su propuesta está diseñada con una arquitectura basada en rondas para el cifrado como para el descifrado y baja latencia para satisfacer las limitaciones de los entornos con recursos limitados. Utilizan dos dispositivos S-boxes, uno de involución y otro de no involución. Las pruebas realizadas fueron ejecutadas en un banco de pruebas (entorno de CAN bus) donde se simula la transmisión de datos cifrados en tiempo real.

Rashad Elhabob et al. [51] proponen un sistema basado en el cifrado de clave pública sin certificado de emparejamiento utilizando prueba de igualdad (CL-PKE-ET). Su enfoque está dirigido a los problemas de confianza y seguridad en los servidores en la nube. Su propuesta permite que los servidores en la nube puedan comparar los datos cifrados y establezcan una igualdad. De esta manera se podrá recuperar e identificar los datos sin la necesidad de procesar los datos cifrados. Los resultados demuestran gran vialidad en entornos cambiantes IoV.

En su artículo, Yun Wu et al. [52] proponen un algoritmo de cifrado en flujo que genera claves pseudoaleatorias basadas en el teorema de Zeckendorf llamado “ZPKG” (Key Generator based on Zeckendorf Presentation). Estipulan que el cifrado en flujo proporciona niveles altos de seguridad. En su propuesta demuestran que la probabilidad de que el número 1 aparezca en la parte media de la representación de Zeckendorf es constante, de esta manera pueden generar claves pseudoaleatorias en flujo. Las claves generadas resultaron tener una fuerte aleatoriedad además son infinitamente largas y robustas ante pequeñas perturbaciones. El algoritmo es utilizado para cifrar datos en el borde de la nube para entornos IoV.

Ling Xing et al. [53] proponen un algoritmo de seguridad basado en la entropía para garantizar la privacidad relacionada con los datos de ubicación en los entornos IoV. En el contexto del Internet Social de los Vehículos (SIoV), el intercambio de datos es propenso a la filtración de datos; por tal motivo, es importante implementar sistemas de protección de datos. En su propuesta,

utilizan la entropía de ubicación para medir la incertidumbre del destino de los usuarios. Entre mayor sea la entropía, mayor será el nivel de seguridad. Posteriormente, las unidades de carretera (RSU) almacenan puntos de interés. De este modo, reducen la sobrecarga del servicio ocasionado por la alta presencia de solicitudes de servicio. En los experimentos, miden la efectividad del algoritmo en "Veins". Los resultados muestran que el algoritmo es capaz de proteger información sobre la ubicación del usuario sin perjudicar el rendimiento del sistema.

Yashar Salami et al. [54] proponen un esquema de descarga segura llamado NSO-VFC para los servicios de Niebla-Nube especiales para IoV. En su investigación, someten su propuesta a un análisis formal e informal frente a ataques activos y pasivos. Para los experimentos utilizaron una herramienta de análisis llamada "Avispa" y simuladores NS3. En las simulaciones se observa un rendimiento favorable utilizando el esquema NSO-VFC, además, existe una mejora en la tasa de entrega de paquetes incluso cuando hay aumento en la densidad de datos en los entornos IoV. Los resultados de desempeño mostraron medidas de seguridad robustas.

De los trabajos anteriores se puede encontrar que el internet de las cosas tuvo un gran impacto en la industria automotriz. Son numerosas las aplicaciones o las áreas de aplicación que pueden existir en estos entornos. Esto ha permitido desarrollar diferentes aplicaciones que son capaces de ofrecer servicios de ubicación, navegación asistida, llamadas de emergencia, monitoreo de unidades, seguros de vehículos, entre otros. No obstante, se ha observado la importancia de adoptar mecanismos de ciberseguridad para salvaguardar la privacidad de los datos de los vehículos. De lo contrario, puede ser muy fácil adquirir, manipular y engañar al sistema de un vehículo para realizar alguna actividad ilícita que puede terminar en un atentado en contra de los usuarios, donde incluso podrían perder la vida

Capítulo 3. Marco teórico

En este apartado se describen los conceptos más importantes que se necesitan para comprender de mejor manera el desarrollo de este trabajo. En primera instancia nos enfocaremos en describir la idea general sobre lo que es el internet de las cosas y cuáles son las diferentes áreas de aplicación que han surgido a lo largo del tiempo como las casas inteligentes, los enjambres de drones, las redes vehiculares, etc.

Se dará especial énfasis en los sistemas que utilizan las redes vehiculares que están basadas en los entornos de internet de las cosas, lo que da origen a lo que hoy conocemos como internet de los vehículos. En esta sección se describirán en qué consiste un sistema de Internet de los vehículos y cuáles son sus limitaciones. Posteriormente se describe cómo funciona un vehículo a nivel informático. También se explicará cuáles son los elementos que intervienen en un vehículo para que este funcione adecuadamente y cómo han evolucionado hasta alcanzar el desarrollo de vehículos con conducción autónoma.

Finalmente, se analizará la importancia que tienen los sistemas de ciberseguridad para proteger información importante en un entorno de Internet de los vehículos. Se describen algunos algoritmos que pueden ser utilizados para obtener un sistema del Internet de los vehículos lo bastante seguro y que propicie a que personas no autorizadas sean incapaces de comprender la información.

3.2. **Internet de las cosas**

En las sociedades modernas el Internet ha jugado un papel muy importante para el desarrollo de nuestras vidas diarias. Es innumerable la cantidad de cosas que se pueden desarrollar con este servicio. Incluso para poder enviar un mensaje se requiere de una conexión a Internet. No cabe duda de que las sociedades modernas se verían incapaces de llevar a cabo muchas actividades sin el internet ya que existe una fuerte dependencia a este tipo de servicios.

Actualmente el Internet se ha distribuido a cada rincón del planeta. Por tal motivo, muchas personas pueden acceder a este servicio incluso de forma gratuita. Además, se puede tener acceso independientemente de la ubicación en la que nos encontremos. Claro está que aún existen muchas zonas sin cobertura, pero ya se está trabajando para cubrir este problema.

Con la distribución del Internet por todo el mundo, muchos dispositivos cotidianos de la vida se han desarrollado tomando en cuenta los sistemas de conexión a Internet. De hecho, no es raro ver alguna lavadora, un refrigerador, dispositivos móviles e incluso un reloj de mano conectado a Internet. Este tipo de implementación se le ha conocido como Internet de las cosas [55].

Implementar un sistema de Internet de las cosas es muy viable y tiene un enorme potencial de uso en los diferentes tipos de servicio o campos laborales (Figura 1). Su uso se puede apreciar en la industria alimenticia, en grandes o pequeñas empresas, en los sistemas de transporte, en los servicios de salud, etc.

Cabe señalar que implementar un sistemas de Internet de las cosas requiere de sus propias características peculiares que dependen del área de aplicación [56]. Es por ello que en muchas ocasiones se le puede llamar Internet del todo, porque el área de aplicación es extensa.

Figura 1. Internet de las cosas

3.3. **Internet de los vehículos**

El auge del Internet de las cosas y su implementación en la industria automotriz, originó lo que hoy conocemos como Internet de los vehículos [57]. IoV surge gracias al reciente avance tecnológico de los vehículos, el aumento de unidades en el mercado y la conectividad avanzada con Internet.

Un entorno IoV es una compleja red vehicular conectada a Internet donde los sensores instalados en los vehículos recopilan e intercambian diferentes datos. Esto permite que la información recopilada (Figura 2) como los datos internos del vehículo, los datos de la infraestructura, los datos del entorno, los datos de visión y detección sean compartidos y procesados con mayor facilidad.

Con IoV se ha logrado que una gran cantidad de vehículos sean conectados a una gran red dónde los automóviles se comunican constantemente entre sí para tomar decisiones de forma automática durante la conducción. Para desarrollar de manera exitosa un entorno IoV, muchas herramientas, aspectos e investigación son requeridas para que los vehículos generen una respuesta adecuada [58].

Figura 2. Internet de los vehículos

Sin embargo, son varios los desafíos que enfrenta esta tecnología lo que ocasiona que no sea tan fácil implementar un entorno IoV en las ciudades inteligentes. Son varios factores como los problemas de gestión de datos, los problemas de escalabilidad, la alta densidad vehicular, la movilidad cambiante, la topología cambiante de la red, la latencia, entre otros; lo que ocasiona que mucha información no se pueda procesar adecuadamente. Además, en los entornos IoV se requiere mucha investigación en temas de ciberseguridad para evitar algún ataque cibernético.

3.3.1. **Elementos y características de los sistemas IoV**

Para poder implementar un sistema IoV requerimos de diferentes elementos que en conjunto forman un sistema completo [59]. En dichos sistemas se pueden distinguir los siguientes elementos.

1. Servicios de nube: La nube es uno de los elementos en la red más importantes para el diseño y desarrollo de un sistema IOV. Prácticamente es el principal elemento donde todos los vehículos deberán conectarse para compartir información. El creciente número de vehículos inteligentes, aunada a la gran cantidad de sensores instalados en los vehículos ha ocasionado que la cantidad de datos recopilados escalen a los petabytes.
2. Redes de comunicación: La red de comunicación es el medio por el cual los vehículos se conectan a la nube. En la actualidad existen varias tecnologías que permiten establecer una conexión a la red para intercambiar información.
3. Vehículos y dispositivos. En IOV los vehículos, los dispositivos personales y los sistemas RSU (por sus siglas en inglés de Roadside Unit) son los principales elementos físicos que conforman un entorno IoV. Estos se conectan a la nube a través de diferentes redes de comunicación.

Asimismo, las principales características que debe tener un ambiente IoV son las siguientes [59,60].

1. Comunicación compleja: Se basa en el intercambio de mensajes a través de diferentes protocolos de comunicación. Los datos provienen de varios sensores que son instalados en los vehículos como los datos GPS, los datos de las cámaras, los datos de los sensores, información de los frenos, estado de la bomba de combustible, entre otros.
2. Topología dinámica: Es la capacidad de adaptación ante cambios repentinos en la topología de la red, por ejemplo, el movimiento a muy alta velocidad por carretera.
3. Alta Escalabilidad: Se refiere a la capacidad de la red para la retención y manejo de información. Debido a la incorporación de nuevas tecnologías, nuevos servicios y al aumento de la densidad vehicular existe mayor cantidad de datos que son generados a cada segundo.
4. Comunicación localizada: Es la capacidad que tiene el sistema para intercambiar mensajes con vehículos cercanos ya sea dentro o fuera de su cobertura geográfica.
5. Energía y capacidad de procesamiento: Es la capacidad que tiene el sistema para procesar información así como la cantidad de memoria de almacenamiento disponible y la capacidad de poder energético de todo el sistema.

3.3.2. **Arquitectura de un sistema IoV**

A nivel informático, la estructura de un sistema IOV consta de cierto número de capas, las cuales varían de acuerdo al autor. Cada una de estas capas se encarga de llevar a cabo alguna tarea específica y de alguna manera, cada una tiene su propio grado de importancia. Algunos ejemplos de arquitecturas del Internet de los vehículos que han sido propuestos por algunos autores se describen a continuación.

Navin Kumar et al. [61] proponen un modelo basado en IoV para detectar anomalías durante la conducción en carreteras. Utilizando la deformación dinámica multidimensional del tiempo (MDTW) para mejorar la puntuación y la sensibilidad de la F1. Su modelo IoV se compone de tres capas clave: la capa de sensores IoT utilizados para recopilar datos, la capa de niebla utilizada para calcular la detección de profundidad y reducir la dimensionalidad de los datos recopilados y la capa de nube que es emplea para archivar los datos históricos.

Kumar et al. [62] presentan un sistema IoV diseñado para vehículos eléctricos. Su enfoque está dirigido en la previsión del consumo de electricidad en un escenario de vehículo a red (V2G). Su sistema se compone de una arquitectura IoV de tres capas. La primera capa es la capa de recopilación de datos, la segunda capa conocida como la capa de niebla, está diseñada para optimizar la eficiencia energética de los dispositivos electrónicos y el análisis de la información. La última capa relacionada con la nube está destinada al almacenamiento de los datos que servirán para pronosticar el consumo.

Liu et al. [63] propone una arquitectura basada en seguridad blockchain llamada HBSSA (del inglés Hierarchical Blockchain-enabled Security threat Assessment Architecture). Su sistema HBSAA consta de 3 capas, que son la capa de percepción, la capa de borde y el centro de datos en la nube. La capa de percepción se encarga de interceptar información proveniente de varios terminales inteligentes como los vehículos, las cámaras, las señalizaciones, etc. Luego la información recopilada se procesa en la capa de borde donde los sistemas RSU aprovechan un sistema de gestión de datos local para evaluar varios escenarios. Finalmente el centro de datos en la nube está formado por diferentes servidores en la nube, este es el medio por el cual se comparte información entre las RSU en diferentes regiones y los vehículos. De esta manera pretenden mejorar la eficiencia al evaluar amenazas a la seguridad de los entornos IoV.

Aroof et al. [64] proponen una arquitectura a la que llamaron CPSN-IoV. Este sistema está compuesto por 5 capas en las que se incluyen: la capa de recopilación de datos, la capa de comunicación, la capa de procesamiento, la capa de fusión de datos y la capa de aplicación. Su objetivo es obtener una arquitectura optimizada para escenarios en tiempo real

Ang et al [65] propone una arquitectura más compleja que consta de 7 capas: la capa de identificación de vehículos, la capa de objetos, la capa de dispositivos, la capa de comunicación, la capa de servidores o servicios en la nube, la capa de procesamiento multimedia o big data y la capa de aplicaciones.

Cada arquitectura propuesta posee sus propias características. Cada una de las capas se encarga de realizar una tarea específica, entre más aumenta el número de capas mayor es la complejidad del sistema IoV. Todas las capas en conjunto se mantienen comunicando entre sí.

3.3.3. **Aplicaciones del Internet de los vehículos**

El auge de los sistemas IoV en las grandes ciudades se debe gracias a la implementación de los sistemas de Internet de las cosas que se han desarrollado especialmente para la gestión de procesos que involucran vehículos. Las aplicaciones del internet de los vehículos tienen una amplia variedad de usos en las que se encuentran [66 - 69]:

a) Aplicaciones basadas en ciudades inteligentes [70]. Los sistemas IoV han sido adoptados de manera satisfactoria en el desarrollo de una ciudad inteligente. Gracias a los vehículos inteligentes es posible implementar una red que se encarga de recopilar una gran cantidad de datos relacionados con el transporte, la gestión de tráfico, la ubicación, la movilidad de los vehículos, el comportamiento del conductor, etcétera. El objetivo es mejorar la calidad de vida y mejorar el entorno de la ciudad.
b) Sistemas de transporte inteligente (Intelligent Transport System): Utiliza aplicaciones IoV basadas en la seguridad que pueden ser utilizados para el aviso de cambio de carril, el aviso del adelantamiento, implementación de sistemas de control automático de velocidad y sistemas de frenado automático.
c) Sistemas de conducción autónoma. Se apoyan por varios sensores instalados en el vehículo como sensores de proximidad, sensores de visión, sensores de radio frecuencia, etc que recopilan información de diferente índole. Los datos son procesados internamente lo que permite al sistema tomar decisiones durante la conducción no asistida.
d) Sistemas de ayuda durante la conducción. Permite que el vehículo interactúe con el entorno para recopilar información. Esto facilita que los vehículos autónomos eviten colisiones o atropellos a peatones. También se encarga de detectar posibles accidentes en carretera.
e) Sistemas de navegación. Permitieron desarrollar aplicaciones destinadas a obtener información en tiempo real sobre los vehículos, la ubicación del automóvil, el seguimiento de vehículos de los miembros de la familia, etcétera.
f) Sistemas de apoyo para puntos ciegos. Permite al conductor monitorear o visualizar el entorno que debido a varios factores, se encuentran fuera del alcance de su vista. Incluso se han hecho estudios para implementar estos sistemas en unidades más pequeñas, como motocicletas o bicicletas.
g) Sistemas ecológicos verdes [71]: Utilizan tecnología de procesamiento avanzado y sistemas energéticos más amigables para reducir la cantidad de residuos o desperdicios generados y disminuir el impacto ambiental.
h) Sistemas marítimos [72]: Utilizados en sistemas de rastreo de ubicación y gestión de tráfico marítimo mediante conexión satelital, redes de acceso de radio (RAN) y redes centrales (CN).

i) Aplicaciones relacionadas con los negocios: Estas aplicaciones se centran en la creación de oportunidades comerciales. En los entornos IOV se pueden generar más valores económicos aprovechando los servicios de alquiler o cobro, los servicios recarga de vehículos eléctricos, tasas de cobro de peajes, cargos por servicios de estacionamiento y servicios de alquiler de vehículos.

3.3.4. **Desafíos en Internet de los vehículos**

La tecnología y los sistemas de automatización han tomado un papel importante en muchas áreas de aplicación en especial en los ambientes IoV. De hecho, gracias a los sistemas IoV se han logrado generar una gran variedad de aplicaciones destinadas a administrar muchos procesos relacionados con la gestión vehicular [73].

Debido a la alta complejidad que poseen los ecosistemas relacionados a los entornos IoV, son muchos los desafíos que se tienen que acatar para lograr que estos entornos ofrezcan mejores servicios. Incluso, con la aparición de nueva tecnología, en un futuro los vehículos generarán más cantidad de datos de diferente categoría, con nuevas características y nuevos requisitos [74]. Estos sistemas aún tienen muchas carencias que deben ser solucionadas antes de implementarlas en las grandes ciudades. Algunos de estos desafíos se enumeran a continuación [75-76].

a) Conectividad con la red [77]: Implementar un sistema IoV requiere de acceso a servicios de Internet. De hecho, aún existen algunas carencias que deben ser tratadas como una conectividad deficiente e inestable, falta de cobertura en zonas remotas y rurales, desfases o desincronización durante el desplazamiento a altas velocidades (modifica la topología del sistema), todos estos problemas generar fallas para que el sistema funcione correctamente.
b) Restricciones de retraso: Esta característica puede ser perjudicial en procesos que requieran altas velocidades de intercambio de mensajes. Por ejemplo, durante una emergencia crítica como el frenado automático ante peligro de colisión, la velocidad de intercambio de mensajes es de suma importancia.
c) Confiabilidad [78]: El entorno IoV debe ser un sistema capaz de intercambiar datos en todo momento, independientemente de las condiciones del entorno. Esta característica permite al sistema asegurar que los datos sean enviados exitosamente al servidor o al centro de control.
d) Alta Escalabilidad: En IoV debe haber un proceso de gestión bien organizado para asegurar la participación de cada uno de los nodos vehiculares que participan en la red.
e) Seguridad y privacidad[79-81]. Los sistemas de seguridad y privacidad tienen un rol de suma importancia para los sistemas IoV. Actualmente es uno de los principales desafíos, por el cual es difícil implementar un sistema IoV. A medida que la tecnología evoluciona y se implementan nuevos dispositivos, hay más cantidad de datos delicados circulando en la red. Estos datos deben mantenerse en completo anonimato y seguros, en especial si ocurre algún percance que pueda afectar directamente la seguridad del usuario.
f) Tolerancia a fallos: Se debe contar con una red de comunicación confiable y a prueba de fallos durante el proceso de comunicación en tiempo real.
g) Servicios sustentables: Se trata de una característica de diseño que permite tener un servicio continuo, fácil, factible y amigable para el vehículo como para el usuario.
h) Falta de estándares: El desarrollo de estándares es una característica muy importante para evitar variaciones durante el proceso de comunicación y procesamiento de datos. La falta de un estándar provoca problemas de implementación, desarrollo e intercambio de información fluida.

3.4. **Vehículos**

Los vehículos a motor fueron una herramienta que revolucionó el estilo de vida de los humanos. Hace unos años para poder mandar artículos o una simple carta, demora varios días e incluso meses en llegar a su destino. Además de la demora de tiempo, existían otros riesgos que afrontar como el extravío de los artículos, el daño a la estructura del objeto o incluso asaltos en carretera durante el traslado.

Con el paso del tiempo, nuevos medios de transporte comenzaron a aparecer. Gracias a estas máquinas, muchas actividades de la vida diaria podían hacerse con mucha más facilidad, seguridad y en menor tiempo.

La tecnología también ha jugado un papel muy importante, pues ha permitido que los automóviles evolucionen de manera desacelerada [82]. Esto se logró con la implementación de una gran cantidad de dispositivos electrónicos que han sido agregados constantemente en el vehículo. De hecho, con la aparición de las primeras computadoras para vehículos y la implementación de los protocolos de comunicación se logró que esta evolución se de aún más rápido pues cada año se logran más avances tecnológicos. Se considera que la mayoría de los inventos automotrices tienen que ver con el desarrollo de hardware y software para los vehículos.

El desarrollo de nuevo hardware permitió grandes avances en muchos sistemas. Simplemente, la implementación de sistemas de gestión de energía mediante batería permitió la incorporación de computadoras especiales para vehículos. La tarea de dichas computadoras dentro del vehículo fue hacer más eficientes, precisos y rápidos muchos de los sistemas del vehículos. Esto marcó

una gran diferencia para los sistemas de control del motor eléctrico, el sistema de transmisión, los convertidores electrónicos de potencia y los dispositivos de almacenamiento de energía.

En la actualidad contamos con muchos medios de transporte sofisticados que permiten agilizar muchos procesos y actividades de la vida cotidiana. La variedad de transporte es extensa pues contamos con medios tan complejos como pueden ser los grandes aviones que pueden atravesar inmensos océanos y trasladar grandes volúmenes de mercancía hasta una simple bicicleta que nos permite trasladar a la escuela o a nuestro lugar de trabajo.

3.4.1. **Tecnología en los vehículos**

La implementación de las computadoras en los vehículos logró grandes avances en la industria automotriz. Gracias a ellas, los vehículos mejoraron sus prestaciones, redujeron el peso del auto y redujeron los precios de producción.

Las computadoras para vehículos conocidas como ECU (del inglés Electronic Control Unit) [83] permiten gobernar y gestionar cada uno de los dispositivos instalados dentro de los automóviles. La cantidad de computadoras que contienen los autos modernos ascienden a más de 50 unidades para vehículos de gama media mientras que en vehículos de alta gama pueden haber más de 100 de estas ECU. La forma en la que se comunican cada una de las computadoras entre sí, se hace a través de un protocolo de comunicación llamado CAN Bus. Incluso, estos protocolos de comunicación redujeron la cantidad de cableado requerido para mantener comunicado a cada uno de los sistemas que conforman un vehículo.

¿Para qué sirve una ecu? Cada una de las ECU [84] tienen la tarea de controlar y gestionar el correcto funcionamiento de los vehículos para que estos realicen diferentes acciones mientras el usuario conduce. Las ECUs son responsables de enviar, recibir, controlar y validar las señales leídas por cada uno de los sensores y tener un rendimiento eficiente del vehículo. Si el funcionamiento de la ECU es incorrecto, puede provocar una falla en el funcionamiento del vehículo.

Las ECUs necesitan conocimiento completo no sólo del rendimiento del motor, sino también datos sobre el comportamiento del vehículo, los parámetros ambientales como la pendiente de la carretera, la resistencia a la rodadura y la resistencia al viento. Todos estos datos son recopilados a través de sensores instalados por todo el vehículo, los cuales serán utilizados para realizar alguna acción.

Algunas de estas computadoras controlan sistemas críticos, como el sistema de frenado o el sistema del motor, mientras que otras controlan sistemas menores, como el módulo de control de cierre y apertura de ventanas. A continuación se mencionan cuáles son los sistemas más importantes según su prioridad.

a) Sistemas primarios: Sistema del motor, asistencia al conductor, línea motriz, sistema eléctrico, sistema de frenado, tablero de instrumentos, etc.
b) Sistemas secundarios: Encendido, indicadores, control de ventanas, limpiaparabrisas, faros, etc.
c) Sistemas de infoentretenimiento: Sistemas de navegación telemática, sistemas de entretenimiento de música y video, servicios basados en GPS, etc.

3.4.2. **Sistemas de un vehículo**

La arquitectura de un vehículo está constituida por un conjunto de sistemas que se encargan de realizar alguna acción específica [85]. Con ayuda de varios sensores y actuadores se realizan un conjunto de mediciones sobre el entorno que rodea al automóvil para que éste desencadene algunos procesos complejos que mantengan en operación al vehículo. El número de dispositivos electrónicos ha aumentado continuamente debido a las nuevas demandas y necesidades que los usuarios tienen con el paso del tiempo.

Figura 3. Sistemas internos de un vehículo

Los sensores junto con los actuadores forman parte de un sistema específico de un automóvil. Los datos recopilados durante el proceso son procesados por las computadoras internas del vehículo y en muchas ocasiones comparten la información con otros sistemas que requieran información específica. Todos estos elementos son necesarios para dar movimiento al vehículo, frenar, dar dirección a las llantas, cerrar o abrir las ventanas, etcétera (Figura 3). Entre los sistemas más importantes de un auto se encuentran los siguientes.

1) Sistema eléctrico y electrónico del vehículo VEE (por sus siglas en inglés de Vehicle Electrical and electronic): Involucra a todos los sistemas y componentes eléctricos y electrónicos utilizados en el vehículo.

    a) Módulo de control de la carrocería BCM (por sus siglas en inglés de Body Control Module: Controla y monitorea diferentes partes eléctricas del vehículo como el aire acondicionado y los espejos eléctricos. La comunicación se realiza a través de los protocolos CAN y LIN.
    b) Administración de energía PMM (del inglés Power Management Module): Administra, proporciona y distribuye energía al sistema VEE.
    c) El módulo de control de puertas y ventanas eléctricas PWDC (del inglés Power Windows and Door Control): Controla la apertura y cierre de las puertas, ventanas, espejos y faros.

d) Entrada de llave remota RKE (por sus siglas en inglés de Remote Keyless Entry): Es el sistema de bloqueo remoto del vehículo. Se puede utilizar para bloquear y desbloquear las puertas de forma remota. Incluso se puede utilizar para arrancar el motor.
e) Espejos y limpiaparabrisas inteligentes SMW (del inglés Smart Mirror and Wipers): Se encarga de activar automáticamente el clima, además ajusta la velocidad del limpiaparabrisas.

2) Electrónica del chasis: El sistema electrónico del chasis contiene elementos que se encargan de controlar varios parámetros. Algunos sistemas del chasis son

a) Sistema de frenos antibloqueo ABS (del Inglés Antilock Breaking System): Da soporte al accionamiento de los frenos para mantener la tracción con la superficie de la carretera y evitar algún bloqueo de las ruedas o resbalones innecesarios en superficies resbaladizas.
b) Sistemas de control de la bolsa de aire ACS (del inglés Airbag Control System): Proteja al conductor y a los pasajeros en el interior del vehículo durante algún accidente.
c) El control electrónico de estabilidad ESC (del inglés Electronic Stability Control): Aumenta la estabilidad de los vehículos al haber una pérdida de tracción.

3) Electrónica de confort: Son dispositivos electrónicos que son instalados en los vehículos para proporcionar confort y entretenimiento a los usuarios.

a) Control climático automático ACC (del inglés Automatic Limit Control): Regula y ajusta la temperatura del habitáculo con respecto al clima exterior.
b) Ajuste electrónico del asiento ESA (del inglés Electronic Seat Adjustment): Gestiona la posición del asiento de cada usuario. También realiza ajustes en los espejos.
c) Ajuste automático del haz de luz ABA (del inglés Auto Beam Adjustment): Ajusta la iluminación de los faros mediante un conjunto de fotosensores durante la mañana y la noche.
d) Ajuste de temperatura: Regula y controla la temperatura del aire acondicionado.

4) Unidades de control electrónico ECU: Son dispositivos compuestos por elementos de hardware/software y se encargan de recopilar y gestionar información del entorno. Actúan en función de los datos obtenidos para activar algunos actuadores que ejecutan alguna acción específica. Los módulos más importantes son:

a) Módulo de control del motor ECM (del inglés Engine Control Module): Se encarga de monitorear y gestionar varias funciones del motor.
b) Módulo de control de la transmisión TCM (del inglés Transmission Control Module): Monitorea y controla el sistema de transmisión así como el cambio de marchas.
c) El módulo de control del vehículo VCM (del inglés Vehicle Control Module): Gestiona varios sistemas del vehículo mediante el procesamiento de información que proviene de varios sensores. Además es el módulo principal del vehículo.

5) Electrónica de Infoentretenimiento. Proporciona medios de soporte a bordo y entretenimiento dentro del vehículo. Los principales sistemas son:

a) El Infoentretenimiento en el vehículo IVI (del inglés In Vehicle Infotainment): Da soporte a los sistemas de audio, reproductores de vídeo y pantallas de visualización.
b) Sistema de audio del vehículo: Proporcionan entretenimiento de música y servicios por comando de voz.

3.5. **Protocolos de comunicación en el vehículo**

Un vehículo convencional contiene una serie de computadoras llamadas ECU a las cuales se les conecta un conjunto de sensores, actuadores y dispositivos electrónicos. Incluso, para hacer funcionar de forma correcta a los automóviles, algunas computadoras se encuentran conectadas a dispositivos externos como equipos digitales, sistemas de entretenimiento, sistemas de navegación, etcétera.

Internamente cada una de las ECU del vehículo se encuentra conectada entre sí mediante una serie de redes de comunicación o protocolos de comunicación [86]. En la actualidad, en un vehículo existen diferentes protocolos de comunicación debido a las diferentes características o requisitos que requieren los diferentes dispositivos instalados en un vehículo. Por ejemplo, se requiere de características como una baja latencia, altas velocidades de intercambio de datos, etc.

Entre los protocolos de comunicación más conocidos se encuentran [87,88].

1) CAN (del inglés Control Area Network): Creado por Robert Bosch en 1986 para la transmisión de datos en los sistemas vehiculares. Actualmente es el estándar más utilizado en la industria automotriz. El CAN (Figura 4) consiste en un par de cables trenzados sin blindaje el cual proporciona una comunicación bidireccional a una tasa de transmisión de hasta 1 Mbps. También tiene la capacidad de detectar errores, posee alta resistencia a interferencias y tolerancia a fallas. Se utiliza para conectar los diferentes dispositivos electrónicos que intervienen en el funcionamiento de un vehículo como los sensores, los actuadores, los microcontroladores y otros dispositivos.

Figura 4. CAN bus en el vehículo

2) FlexRay: Fue desarrollado por un consorcio formado por empresas de la industria automovilística. El Bus FlexRay es un protocolo de comunicación flexible y tolerante a fallas. Proporciona velocidades de transmisión de datos de hasta 10 Mbps. Este protocolo es resistente a errores de comunicación, procesos de verificación de redundancia, codificación y decodificación. Suele utilizarse en aplicaciones críticas donde la velocidad de transmisión debe cumplir con un marco de tiempo estricto.
3) LIN (del inglés Local Interconnect Network): Es utilizado ampliamente en la industria automotriz debido a su bajo costo de implementación. Utiliza software sencillo de implementar y un solo arnés de cable flexible. Sin embargo, su inconveniente es que la velocidad máxima de transmisión es de 20 kbps. La primera implementación del protocolo LIN se dio en noviembre del 2002.
4) Ethernet automotriz AE (del inglés Automotive Ethernet): Es una reciente tecnología de transmisión dúplex que es capaz de ofrecer velocidades de transmisión de hasta 100 megabytes por segundo. El AE tiene mejores características de seguridad que están basadas en esquemas de enrutamiento IP, además posee baja latencia y aumenta el rendimiento de los datos. El AE es capaz de evitar ataques de ciberseguridad gracias a sus protocolos de seguridad.
5) Most (del inglés Media Oriented System Transport): Permite implementar sistemas de infoentretenimiento y la transmisión de datos de audio, vídeo y voz.
6) Transmisión nibble de borde único SENT (del inglés Single Edge Nibble Transmission): Es un protocolo de comunicación que permite intercambiar señales desde un sensor o un controlador. Está basado en un protocolo de comunicación de punto a punto.
7) Señalización diferencial de bajo voltaje LVDS (del inglés Low Voltage Differential Signaling).

3.6. **Vehículos conectados**

En los vehículos modernos existe una gran variedad de sensores y actuadores que están gobernados por una computadora. Estos dispositivos generan una gran variedad de datos a cada segundo los cuales serán intercambiados con otros sistemas para que el vehículo comience a funcionar.

Nuevas tecnologías usadas en el intercambio de información entre las ECU del vehículo y los dispositivos externos, la conexión a Internet y el auge de los vehículos inteligentes propició el uso de nuevos mecanismos de comunicación en un vehículo. Estos mecanismos están pensados para facilitar los procesos de intercambio de información entre los autos y la infraestructura. En muchas ciudades desarrolladas, los vehículos ya poseen conexión inalámbrica con otros vehículos, con la infraestructura y con los servicios en la nube. A este tipo de tecnología se le conoce como tecnologías de vehículos conectados CV (del inglés Connected Vehicle) [89].

Las CV están basadas en redes ad hoc que permiten la comunicación con otros nodos que participan en la red. A est redes de conexión se les conoce como redes VANET. Los avances con los sistemas VANET permiten que los vehículos inteligentes intercambien información relacionada con el vehículo y el entorno exterior para prevenir accidentes, dar asistencia de conducción segura, analizar la congestión vehicular, localizar zonas de construcción y proveer entretenimiento multimedia en el vehículo. Esta tecnología es clave para el desarrollo de vehículos inteligentes y automóviles autónomos [90, 91].

Las VANETS [94,95] también permiten la comunicación con vehículos vecinos, infraestructura, redes centrales, peatones, ciclistas, entre otros. La comunicación en las redes VANET se da de forma inalámbrica y se puede lograr mediante.

1) Comunicación vehículo a infraestructura V2I (del inglés Vehicle to Infrastructure): Está destinado a facilitar el intercambio de información que puede ser recopilada de la infraestructura. En comunicaciones V2I los vehículos se conectan a unos dispositivos que pueden encontrarse en carretera llamados unidades de carretera RSU (por sus siglas en inglés de On Roadside Units).
2) Comunicación vehículo a Red V2N (del inglés Vehicle to Network): Se refiere a la conexión inalámbrica o celular con los servidores remotos y servidores basados en la nube.
3) Comunicación vehículo a vehículo V2V (del inglés Vehicle to Vehicle): Posibilita la conexión con otros vehículos cercanos.
4) Comunicación vehículo a peatón V2P (del inglés Vehicle to Pedestrian): Admite la conexión en modo ad hoc con los peatones o ciclistas vulnerables en la carretera.
5) Comunicación vehículo a todo V2X (del inglés Vehicle to Everything).

3.7. **Vehículos autónomos**

Los vehículos autónomos [96] tienen origen aproximadamente hace 20 años y a lo largo de estos años, la industria automotriz ha generado mucha investigación para aumentar la eficiencia y la seguridad de los vehículos. La conducción autónoma es una realidad gracias a la implementación de múltiples sensores que miden señales internas como externas, aprovechan los sistemas de navegación y hacen uso de sistemas relacionados con el Internet de las cosas o internet de los vehículos [97]. También hacen uso de métodos de procesamiento inteligente de datos como el aprendizaje automático o machine learning para procesar datos en tiempo real, y realizar alguna acción durante la conducción, como la evasión de obstáculos. La conducción autónoma es muy compleja ya que son muchas las herramientas especializadas que se necesitan para procesar y analizar toda la información recopilada y tomar decisiones importantes durante la conducción (Figura 5).

Figura 5. Vehículos autónomos

Las tecnologías de conectividad también forman parte importante en la conducción autónoma, lo que permite la comunicación entre vehículos con su entorno. Estas conectividad dependen en gran medida de las redes VANET, las cuales establecen una constante comunicación con cada uno de los participantes de la red. En especial para que un vehículo sea capaz de conducir de forma autónoma sin intervención humana.

El objetivo de un sistema autónomo [98, 99] o lo que se busca es conseguir varios beneficios sociales y ambientales entre los que se incluyen: mayor eficiencia del tráfico, mayor inclusión y accesibilidad, reducción de emisiones, seguridad durante la conducción, servicios seguros y convenientes para usuarios que sufren síntomas de estrés relacionado con la conducción prolongada, transportar personas con problemas de movilidad y minimizar los accidentes [100]. Estadísticamente se estima que cada año se producen aproximadamente 1,35 millones de muertes y entre 20 y 50 millones de lesiones no mortales causadas por accidentes de tráfico (Organización Mundial de la Salud, 2022). En México, durante el 2022 se registraron aproximadamente 377,231 accidentes viales (INEGI 2022).

En los vehículos modernos, el funcionamiento del sistema autónomo se encuentra dividido primordialmente por 2 fases de conducción. La primera fase se enfoca en la conducción asistida, mientras que la segunda fase se centra en la conducción autónoma sin ninguna clase de intervención o interacción humana. En la segunda etapa es donde las tecnologías de conectividad, los sistemas de comunicación, los dispositivos electrónicos como los sensores, tienen mayor participación. Dependiendo de las variables leídas en el entorno, el vehículo circulará de forma autónoma sin ningún percance.

¿Cómo se obtienen las variables del entorno? Estas son obtenidas gracias a la gran variedad de sensores instalados en los vehículos con los cuales se puede detectar obstáculos, peatones, semáforos, vehículos cercanos, etc [101].

Con los datos obtenidos por los diferentes sensores que intervienen en el funcionamiento de un automóvil se inicia el procesamiento de la información. Derivado de que existe una gran cantidad de fuentes de datos, la fusión de sensores [103] toma un rol importante. Esta técnica es utilizada para combinar información que se obtuvo de diferentes sensores.

3.7.1. **Tecnologías de conducción autónoma**

Un vehículo autónomo puede ser visto como un gran sistema que está compuesto por múltiples sensores. Dichos sensores en conjunto con herramientas de procesamiento de datos pueden recopilar, procesar y analizar información en tiempo real para ejecutar alguna acción como la detección de obstáculos, la evasión de peatones, etc. En un vehículo autónomo son muchos los sistemas que incorporan este principio y son conocidos como sistemas avanzados [104].

Estos sistemas consisten en dispositivos inteligentes que proporcionan información de diferentes ámbitos como el tráfico, advertencias de colisión, detección de obstáculos, sugerencias de ruta, detección de cambio de carril, frenado de emergencia, entre otros. También permiten la comunicación entre vehículos cercanos, la comunicación con la infraestructura y la comunicación con centros de gestión de tráfico. Algunos alertan al usuario sobre situaciones peligrosas o simplemente toma el control del vehículo ante la falta de atención del usuario o ante una respuesta tardía por parte del usuario.

A continuación se muestran algunas de las tecnologías más importantes en la conducción autónoma.

a) Detección y alcance de luz LIDAR (del inglés Light Detection And Ranging): Consiste en dispositivos láseres y escáneres que utilizan un haz de luz para localizar e identificar objetos cercanos al vehículo. Estos sistemas pueden generar información 3D de un área particular para proporcionar detección remota.
b) Cámaras: Utilizan diferentes tipos de cámaras como las infrarrojas, visión nocturna y cámaras de seguimiento para monitorear variables tanto del exterior como del interior, por ejemplo, el comportamiento del conductor.
c) Detección y alcance por radio Radars (el inglés Radio Detection and Ranging): Son un conjunto de sensores que tienen como objetivo detectar otros obstáculos. Su alcance es de más de 200 m de distancia y son resistentes a varias condiciones climatológicas.
d) Control de crucero Adaptativo ACC (del inglés Adaptive Cruise Control): Gestiona los cambios de velocidad del vehículo para mantener distancia con otros vehículos cercanos.
e) Frenado automático de emergencia AEB (del inglés Automatic Emergency Braking): Gestiona la respuesta de los frenos para reducir velocidad, frenar el vehículo o evitar colisiones.
f) Monitoreo de puntos ciegos BSM (del inglés Blind Spot Monitoring): Monitorea la cercanía de los automóviles que vienen por detrás o por los carriles laterales. Utiliza sensores colocados estratégicamente para cubrir puntos ciegos y advertir al conductor sobre la presencia de un vehículo cercano. La forma de advertir se realiza mediante indicadores colocados en los retrovisores exteriores.
g) Advertencia de colisión frontal FCW (dale inglés Forward Collision Warning): Monitorea automóviles cercanos que van a gran velocidad o que están estacionados. Su objetivo es prevenir una posible colisión.
h) Advertencia de cambio de carril LDW (del inglés Lane Departure Warning): Detecta los marcadores de separación del carril sobre la carretera. En función del comportamiento del conductor alerta sobre cambios repentinos o involuntarios de carril.
i) Asistencia para mantenerse en el carril LKA (del inglés Linkoping Assist): Sirve como sistema de apoyo para mantenerse o regresar al carril. Si el conductor no tiene alguna reacción adecuada, el sistema LKA devolverá el vehículo al centro del carril.

3.8. **Importancia de la ciberseguridad en los vehículos**

La implementación de funciones avanzadas [105] en los vehículos lograron que los autos sean cada vez más inteligentes y autónomos. Las unidades modernas y completamente autónomas envían y reciben una gran cantidad de datos que son recopilados por diferentes sensores, vehículos cercanos, infraestructura, peatones, señales en carretera, etc.

No obstante, al existir una gran cantidad de datos que pueden ser muy importantes aunado a la carencia de sistemas de seguridad que protejan la red de un vehiculo, esto propicia que los hackers se vean atraidos a violar el sitema para obtener alguna ventaja significativa o incluso perjudicar al propio sistema como atentar contra el usuario.

La implementación de nueva tecnología solo agrava el problema ya que es susceptible a sufrir diversos tipos de ataques, sin embargo, existen muchas herramientas que pueden dar protección a los sistemas del vehículo ya sea de manera local como el CAN bus o de manera remota vía internet.

3.9. **Ataques de ciberseguridad a los sistemas vehiculares**

Como en cualquier sistema informático existen ambientes que son susceptibles a recibir ataques de ciberseguridad. Estos ataques podrían comprometer y dañar algunos procesos que afecten la estabilidad y solidez del sistema [108,109]. En el caso del mundo de los vehículos en general y los entornos del Internet de los vehículos, los ataques que se pueden realizar son:

a) Ataques de autenticación: Tienen el objetivo de obstaculizar la autenticación de los vehículos lo que dificulta la identificación de la información recibida por otro vehículo cercano. Algunos de los ataques de autenticación más conocidos son los ataques tipo sybil, ataques de enmascaramiento (Impersonation), ataques de suplantación (phishing) con los cuales se crean múltiples identidades virtuales. Algunas de las soluciones a estos ataques son los sistemas criptográficos basados en identidad (IBC), las firmas digitales, los dispositivos a prueba de manipulación (TPD), técnicas de intercambio secreto multiplicativo (MSS), etcétera.
b) Ataques de disponibilidad: Este tipo de ataques perturban la disponibilidad del sistema durante la comunicación o hacen que los recursos no estén disponibles. En estos casos se interrumpe la comunicación inalámbrica entre los vehículos y la infraestructura. Ejemplos de ataques de disponibilidad son el ataque de interferencia de canal, el ataque de denegación de servicios DoS (del inglés Daniel of Service), el ataque DoS distribuido (DDoS), ataques destinados a dificultar el intercambio de información (Selfish Attack), ataques de cambio de enrutamiento (Routing) actualizaciones maliciosas (Rouge Update).
c) Ataques de integridad: Ocurre cuando se agrega o modifica información durante el proceso de comunicación. Algunos de los ataques de integridad son el ataque de supresión de mensaje (Message supresión Attack), los ataques de ilusión (Illusion Attack), los ataques de sincronización (Timing Attack), los ataques de secuestro de sesión (Session Hijacking Attack), los ataques de confianza (Trust Attack), los ataques de inyección y validación de mensajes falsos (Spoofing), los ataques de inyección de mensajes aleatorios (Fuzzy Attack) y los ataques de falsificación de datos (Falsifying).
d) Ataques: Este tipo de ataque tiene como objetivo obtener y procesar datos de la red. Si los sistemas de seguridad son deficientes, puede llegar a revelarse la identidad del vehículo, la identidad del propietario, contraseñas, códigos de acceso u otra información del vehículo. En casos extremos, esto permitirá tomar el control del vehículo para causar daño a los ocupantes. Entre los ataques más conocidos tenemos el ataque de escucha ilegal el cual es muy difícil de rastrear, el robo de información (eavesdropping), los ataques de manipulación de datos (MITM o man-in-the-Middle-Attack).
e) Ataques de control de acceso: Permiten acceder al sistema para robar credenciales y hacerse pasar por un vehículo legítimo para realizar alguna actividad maliciosa. Algunos ejemplos de ataques de control de acceso son los ataques de diccionario (Dictionary Attack), la reproducción de datos (Replay Attack) y los ataques de fuerza bruta (Brute Force Attack). Entre las soluciones para prevenir este tipo de ataques encontramos las restricciones de acceso al sistema, las políticas de acceso mediante contraseñas o definir políticas de bloqueo ante algún acceso no autorizado.

3.10. **Ciberseguridad**

Los vehículos modernos necesitan mucha información para poder funcionar correctamente, actualmente, son muchos los dispositivos involucrados que se encargan de conseguir esta información. En general, son 3 los elementos que conforman una red de intercambio de información dentro del vehículo, estos dispositivos son principalmente las computadoras, los sensores y los protocolos de comunicación. Los sensores se encargan de medir varias variables, las computadoras se encargan de procesar la información y los protocolos de comunicación permiten el intercambio de información entre los diferentes dispositivos.

Sin embargo, como sucede en una red de computadoras convencional, una gran cantidad de casos de ataque pueden ser ejecutados. Incluso, con el rápido crecimiento del número de vehículos inteligentes y los vehículos autónomos, la cantidad de datos generados en los ambientes IoV aumenta [111]. Por tal motivo, existe un alto riesgo de seguridad en el intercambio de información que solo va en crecimiento ya que diversas formas de ataques surgen con el paso del tiempo. Esto se agrava aún más cuando sabemos que un vehículo no implementa mecanismos de seguridad de datos, lo que ocasiona que existan muchas vulnerabilidades y que muchos activos pueden verse comprometidos.

A largo plazo, las vulnerabilidades pueden ser aprovechadas por entidades maliciosas que buscan algún beneficio. Una entidad maliciosa puede ser desde una sola persona hasta un grupo de personas o software que buscan encontrar una vulnerabilidad en el sistema. Su objetivo final es hacer que el sistema colapse, se dañe, tome el control o simplemente que se abra una puerta de acceso para obtener datos del sistema.

Es por ello que los sistemas de seguridad se han vuelto una herramienta indispensable en el desarrollo de nueva tecnología. Con los mecanismos de seguridad [113] se busca dar protección a los activos críticos en el sistema contra amenazas maliciosas. También se busca mitigar el impacto de un ataque en caso en el que el ataque haya tenido éxito.

En ciberseguridad existen estándares o modelos que pueden ser utilizados para calificar un sistema dado. Un sistema será lo suficientemente robusto si se logra cumplir con algunos de los servicios de la tríada CIA [114, 115]. Dicha tríada corresponde con los servicios de confidencialidad, la integridad y la disponibilidad para dar protección a un sistema.

a) Confidencialidad: Garantiza que los activos críticos sólo estarán disponibles para los usuarios autorizados.
b) Integridad: Garantiza que los usuarios no autorizados sean incapaces de modificar, alterar o manipular la información durante el proceso de transmisión.
c) Disponibilidad: Garantiza que los datos estén disponibles cuando el usuario los requiera.

Otra triada que se puede contemplar es la AAA. Este modelo contempla los servicios de autenticación, autorización y responsabilidad. Su uso tiene más impacto en sistemas de control de acceso a los recursos prioritarios.

a) Autenticación: Implementa mecanismos de validación de identidad para validar solicitudes de entrada al sistema.
b) Autorización: Aprueba y otorga privilegios para realizar alguna operación específica.
c) Responsabilidad: Proporciona la capacidad de monitoreo de las actividades que los usuarios han realizado dentro del sistema. También permite evaluar qué servicios se han utilizado y cuántos recursos se han consumido.

3.11. **Vulnerabilidades y ataques**

En los sistemas donde existen grandes cantidades de datos y en especial donde se maneja información delicada, normalmente los hackers buscan alguna vulnerabilidad [116] para realizar algún ataque y obtener un beneficio. Por lo general, los sistemas son vulnerables y propensos a diferentes tipos de ataques. El término vulnerabilidad se refiere a la nula capacidad de resistencia ante un fenómeno amenazante. Incluso en muchos casos no se tiene la capacidad de responder después de que ha ocurrido algún ataque.

3.12. **Medidas de ciberseguridad**

Existen diferentes herramientas que permiten evitar, contraatacar o mitigar una gran cantidad de vulnerabilidades para proteger el sistema ante amenazas. Incluso estas herramientas son de gran utilidad cuando ya se ha logrado realizar un ataque con éxito. Muchas de estas herramientas tienen una complejidad bastante elevada para detectar intrusiones en tiempo real. Para lograr esto, se utilizan distintos métodos de análisis de datos como inteligencia artificial, deep learning, machine learning, redes neuronales, etc. Con ellas se pueden mejorar las estrategias de defensa, mitigar amenazas potenciales y garantizar la seguridad de los sistemas objetivo [117].

A continuación se describen algunos mecanismos utilizados en ciberseguridad para proteger diversos sistemas. Entre las herramientas más utilizadas tenemos por ejemplo[118]:

- Firewalls que gestionan y dan acceso solo a aquellas entidades autorizadas
- IDS e IPS que monitorean los datos internos en una red dada para ver si existe alguna actividad sospechosa
- Honeypot que permiten recolectar información sobre algún ataque que haya sido realizado
- Sistemas criptográficos que protegen datos que circulan en la red
- Sistemas blockchain que pueden actuar como una base de datos confiable e inmutable para el análisis forense en casos de accidentes

3.14. **Criptografía**

La criptografía [123] es una ciencia que se encarga de dar seguridad y protección a los datos que son intercambiados o compartidos en un sistema dado. Utiliza la teoría de las matemáticas para procesar información y modificar el texto, de tal modo que nadie pueda comprender el contenido. Dicho mensaje sólo podrá ser comprendido a menos que la persona indicada tenga en su poder información adecuada que le permita descifrar el mensaje y ver el contenido original.

Normalmente, en un sistema criptográfico existen 2 entidades que quieren enviarse mensajes entre sí pero quieren evitar que una entidad externa comprenda dicho mensaje. Las entidades mencionadas anteriormente se denominan como emisor y receptor (Figura 6). Existe una tercera entidad que también es conocida como Hacker.

Figura 6. Criptografía en el proceso de comunicación

El objetivo del emisor y del receptor es intercambiar mensajes de forma segura sin que el contenido sea comprometido. La tarea del hacker es vulnerar el sistema para interceptar y comprender el contenido de tal forma que obtenga alguna ventaja.

En ambos escenarios es necesario que las personas involucradas tengan nociones sobre la teoría de las matemáticas. Específicamente el emisor hará todo lo posible para proteger los datos mientras que el hacker empleará herramientas que le permita interceptar y leer mensajes.

3.14.1. **¿Cómo funciona la criptografía?**

Para comenzar debemos tomar en cuenta que en la mayoría de los casos, los medios por los que podemos intercambiar información son de origen público, es decir, cualquier persona externa puede acceder a ellos. El objetivo es lograr que dicha persona externa sea incapaz de ver el contenido del mensaje [124].

Para comprenderlo de mejor manera, supongamos que tenemos un sistema con 2 personas “A” y “B” y ambos quieren intercambiar información entre sí. Si “A” envía un mensaje a “B” por ejemplo, la palabra “hola”, dicho mensaje no puede enviarse como tal ya que una persona desconocida podría interceptar el mensaje y leer el contenido del mensaje. En su lugar “A” tendría que enviar algo diferente para que posteriormente “B” procese la información y obtenga el mensaje original que es “hola”.

La forma en que se debe intercambiar el mensaje de forma segura y que el receptor puede recuperar el mensaje es mediante el acuerdo de un protocolo, contraseña o llave secreta. En este punto es donde la criptografía comienza a trabajar, para ello “A” utiliza algoritmos criptográficos que modifican el mensaje. Por su parte, el receptor sólo será capaz de recuperar el texto original con la llave adecuada que fue acordada o compartida durante el proceso. Por otro lado, la persona que no participó en dicho proceso será incapaz de recuperar el texto original, pues no supo cómo se modificó la información.

3.14.2. **Terminología en la criptografía**

En el proceso de cifrado de un texto intervienen varios elementos [124]. Cada uno tiene una tarea específica que tiene que ser realizada. Para poder identificar cada uno de estos elementos, en la criptografía se emplean los siguientes términos:

- Texto claro o “plaintext” que hace referencia al mensaje original que se desea compartir. También se la conoce como texto sin formato.
- Mensaje cifrado o “ciphertext” hace alusión a la información que ya fue cifrada. Esta información alterada es la que será compartida y enviada por los diferentes canales de comunicación existentes.

En criptografía, para poder distinguir entre el texto plano y el texto cifrado es mediante el uso de letras minúsculas y letras mayúsculas. Para el texto sin formato se usan las letras minúsculas y para el texto cifrado utilizaremos las letras mayúsculas, por ejemplo:

Texto en formato: la criptografía es interesante

Texto cifrado: ET ARVQITCRJAEF KU HWPAHXFMWVI

Para utilizar los algoritmos de cifrado que se encargan de realizar los procesos matemáticos que modifican la información necesitamos algunos componentes importantes. Específicamente necesitamos 2 elementos que nos permitan generar el texto cifrado a partir del texto plano y viceversa. Estos son el protocolo o criptosistema y una clave específica también conocida como llave. Un criptosistema consta de 3 algoritmos, el algoritmo de cifrado, el algoritmo de descifrado y el algoritmo de generación de llaves.

a) Algoritmo de cifrado: Se encarga de convertir el texto sin formato en texto cifrado. Dicho algoritmo utiliza una llave para cifrar el mensaje.
b) Algoritmo de descifrado: Tiene la tarea de procesar el texto cifrado y generar el texto original. De igual manera, en este algoritmo se utiliza una llave para descifrar.
c) Llave de cifrado: Es la clave utilizada para cifrar el texto sin formato.
d) Llave de descifrado: Es la clave utilizada para descifrar y obtener el texto original.

En algunos casos la llave de cifrado como la de descifrado son las mismas y en otro se utiliza una llave pública y una privada completamente diferentes pero que tienen una correlación matemática entre sí.

Por último tenemos el término criptoanálisis el cual se refiere al estudio y análisis de mensajes cifrados. En otras palabras es el proceso de transformar datos cifrados a texto original.

3.14.3. **Esquemas de cifrado**

Los algoritmos criptográficos suelen utilizar un conjunto de elementos para cifrar datos. Entre estos elementos las llaves juegan un papel muy importante [124] y en consecuencia, se han establecido diferentes esquemas para manejar estos elementos. En general, contamos con los siguientes esquemas: “cifrado simétrico” y el “cifrado asimétrico”

Cifrado simétrico: Utiliza una sola llave para el proceso de cifrado como para el descifrado. Dicha llave no debe ser compartida con terceros y debe estar completamente resguardada. Matemáticamente utiliza la sustitución y la permutación para modificar el texto. Entre estos algoritmos podemos destacar los siguientes:

- Cifrado en bloques: En este cifrado el texto se procesa en bloques, grupos de bits o grupos de palabras. El tamaño del bloque está estipulado normalmente por un algoritmo específico. Por ejemplo, el algoritmo de cifrado DES agrupa los datos en bloques de tamaño de 64 bits. En el algoritmo de cifrado AES se utilizan bloques con un tamaño mínimo de 128 bits y un máximo de 256 bits.
- Cifrado en flujo o Stream Cipher. El texto original es procesado bit a bit, es decir, en cada instancia un solo bit del texto sin formato es procesado. Como consecuencia se genera un bit de texto cifrado.

Cifrado asimétrico: Utiliza un par de claves para cifrar y descifrar. Normalmente se genera una llave privada y a partir de ella se genera la llave pública. Sin embargo es imposible generar la llave privada de la llave pública. Ambas llaves son diferentes entre sí pero tienen una fuerte relación matemática.

El proceso de cifrado y descifrado en un esquema de cifrado asimétrico es más lento. Eso se debe a que la longitud de la llave es más grande.

3.15. **Algoritmos de cifrado**

La criptografía [125] ha sido utilizada como método de protección de datos desde la antigüedad, incluso hay indicios de su uso que datan desde hace más de 4000 años. Un ejemplo muy simple y relativamente antiguo consistía en escribir mensajes en tiras de piel, las cuales deben ser enrolladas en un tubo con ciertas características (diámetro específico) para poder ver el mensaje original.

Con la aparición de las computadoras, los algoritmos de cifrado comenzaron a ser de suma importancia, en especial si había mucho intercambio de información personal. Uno de los primeros algoritmos en aparecer fue el cifrado César. Estos algoritmos eran relativamente simples y conforme avanzaba la tecnología se volvían cada vez más obsoletos. En la actualidad existen diferentes algoritmos que permiten cifrar información para compartirla de manera segura en un ambiente abierto. Algunos algoritmos conocidos son:

- Cifrado César
- Cifrado Vigenère
- Cifrado DES
- Cifrado AES
- Cifrado RSA

El proceso general que se lleva a cabo para cifrar información es de la siguiente manera.

1. Se preparan los algoritmos de cifrado.
2. Se generan las llaves.
3. La llave pública se pone a disposición de cualquiera que la requiera.
4. La llave privada se almacena y se mantiene en completo secreto.
5. El remitente obtiene la llave pública y cifra los datos con la misma.
6. El remitente transmite los datos.
7. El receptor usa la clave privada para descifrar el mensaje.

3.15.1 **Cifrado César**

Este algoritmo fue uno de los primeros en aparecer. Realiza un procesos matemáticos muy simples, prácticamente realiza un intercambio de letras. En dicho algoritmo se puede intercambiar la letra del mensaje original por otra que aparece 3 posiciones después en el alfabeto. Por ejemplo, cada letra “A” se intercambiaba por una “D”, cada letra “B” se convierte en una “E” y así sucesivamente. También debemos tomar en cuenta que al llegar a la letra “Z” el alfabeto se reinicia por lo que cada letra “X” se convierte en una “A”, cada “Y” se intercambia por una “B” y cada “Z” se sustituye por una “C”.

Ejemplo:

hola mundo → KROD OXPGR

Para obtener el mensaje original, el receptor debe conocer cómo se realizó el cifrado, es decir, tiene que saber el número de posiciones que se desplazaron las letras para que sea capaz de descifrar la información. Ejemplo.

KROD OXPGR → Hola mundo.

Más tarde los algoritmos por sustitución comenzaron a reemplazar el algoritmo César ya que este último mostró problemas de seguridad y fácil de descifrar. Generalmente el cifrado por sustitución es más difícil de descifrar, sin embargo, pueden ser descifrados mediante fuerza bruta.

Una alternativa para mejorar los algoritmos de cifrado por su institución fue utilizar una palabra clave y además se debe evitar la repetición de letras. Para configurar esto se elige la palabra clave, posteriormente agregamos la palabra clave al inicio del alfabeto y se eliminan las letras repetidas. Esta es una permutación de las letras del alfabeto y sirve como clave. Por ejemplo si la palabra clave es “clave” obtendremos los siguiente:

Tabla 6. Ordenamiento del abecedario con palabra clave para el cifrado César

Eso significa que si ahora tenemos la letra “a” debemos sustituirla por una letra “c”, la letra “b” se sustituye por una “l”, la letra “c” se cambia por una “a” y así sucesivamente. Ejemplo.

hola mundo → FNJC KTMVN

3.15.2. **Cifrado Vigenère**

El cifrado por sustitución anterior ha mostrado vulnerabilidades. Incluso con un análisis de frecuencias se puede llegar al mensaje original. En consecuencia, otros algoritmos de cifrado más potentes fueron propuestos como el cifrado polialfabético. Existen muchas formas de configurar un cifrado polialfabético. El más famoso es el de cifrado vigenère [125]. Este algoritmo solía considerarse fuerte, sin embargo, después de aproximadamente 300 años de uso se descubrieron vulnerabilidades.

La forma en que funciona el cifrado vigenère es mediante la sustitución de cada letra por una entidad específica. En esta ocasión se utiliza una tabla de codificación llamada tabla recta. Asimismo, es necesario seleccionar una palabra clave. Una característica de este tipo de cifrado es la simetría de la tabla, ya que no importa cuál es la clave y el texto plano, pues siempre obtendremos el mismo resultado.

Tabla 7. Tabla recta para el cifrado Vigenère

Supongamos que alguien desea cifrar la frase “probando el algoritmo v” y se elige como palabra clave “Clave”. Posteriormente se realiza la codificación del mensaje. El proceso seguido para obtener el texto cifrado con el algoritmo vigenère fue el siguiente. En primer lugar, dividiremos el mensaje original en bloques de cierto tamaño. Generalmente, en la criptografía, el texto suele dividirse en 5 bloques. Posteriormente calculamos el texto cifrado, esto se logra usando la letra “c” como clave para la primera letra “p”, la letra “l” como clave para la segunda letra “r”, la letra “a” como clave para la tercera letra “o”, y así sucesivamente.

Table 8. Texto plano y clave para el cifrado Vigenère

Tabla 9. Texto cifrado con el algoritmo Vigenère

Para hacer el proceso de descifrado debemos conocer la palabra clave. Si alguien recibe el mensaje anterior y conoce la palabra clave, este podrá descifrar el mensaje de la siguiente manera. El primer carácter en el texto cifrado es la letra “R”, la primera letra de la clave es “c”. Para descifrarlo, ubicamos la columna que contenga la letra “c” e identificamos la letra “R” en toda la columna. De esta manera encontramos que la “R” aparece en la fila “p”, entonces la primera letra del texto claro será la letra “p”. Este proceso se realiza para cada una de las letras del texto cifrado hasta que obtengamos el mensaje original.

3.15.3. **Cifrado AES**

Dadas las desventajas de los algoritmos anteriores se han desarrollado nuevos métodos más complejos que implementan mejores características como el uso de llaves más complejas y procesos matemáticos más laboriosos. El algoritmo AES por ejemplo, es un algoritmo de cifrado simétrico, es decir, ya requiere de una llave para cifrar y descifrar un mensaje.

Para cifrar los mensajes se desarrollan una serie de operaciones que permiten modificar el texto que queremos proteger. De esta manera, alguna entidad no deseada será incapaz de comprender el mensaje. El proceso que se sigue en el cifrado AES inicia desde la elección del texto que queremos cifrar. Debemos tener en cuenta que el texto debe estar en código hexadecimal, de lo contrario, hay que realizar la conversión correspondiente. Asimismo, el texto ya convertido debe estar estructurado en una matriz de tamaño 4x4.

También hay que generar una llave con una longitud específica que va desde los 128 bits hasta un máximo de 256 bits. De igual manera, esta llave debe estar en forma de matriz de 4x4. Una vez que obtenemos las matrices del mensaje como el de la clave, comenzamos a realizar las operaciones necesarias. El proceso de cifrado en el algoritmo AES se encuentra dividido en 2 partes.

a) El cálculo de la subclaves
b) Proceso de cifrado.

3.15.4. **Cifrado RSA**

El nombre del algoritmo RSA proviene de las iniciales de sus creadores Rivest, Shamir y Adleman. Se trata de un algoritmo de cifrado asimétrico que utiliza 2 llaves para cifrar y descifrar los datos, la llave privada y la llave pública. Todo contenido que fue cifrado con la clave pública podrá ser descifrado con la llave privada y viceversa. Actualmente el tamaño para generar las llaves RCA se estipula desde un mínimo de tamaño de 1024 bits hasta un máximo de 4096 bits de tamaño.

Este protocolo basa su funcionamiento en el cálculo de logaritmos discretos mediante números primos muy grandes y también aprovecha la complejidad para factorizar números compuestos. Para su implementación, el algoritmo se encuentra dividido nuevamente en 2 etapas.

a) Etapa de generación de llaves.
b) Está padre cifrado y descifrado.

Capítulo 4. Desarrollo e implementación

En este apartado se describe la metodología utilizada para desarrollar el presente trabajo. Así mismo, se da una breve descripción sobre las herramientas que se utilizaron y cuáles fueron algunas de las consideraciones que se tuvieron en cuenta para implementar este proyecto.

Posteriormente se describe cómo se desarrollaron algunos de los experimentos para tener un sistema IOV que contenga herramientas de protección de datos para asegurar que la información compartida en dicho ambiente sea completamente segura e incomprensible para terceros.

4.2. **Metodología**

En este apartado se abordará la metodología utilizada durante este proyecto. En la Figura 7 se observa la estructura completa de dicha metodología. De manera general esta propuesta contempla 7 etapas. La primeras etapas corresponden con la definición de un sistema IoV y el uso de un simulador de un sistema CAN bus de un vehículo, el cual permitirá simular datos de un vehículo. Posteriormente se contempla la etapa de algoritmos de procesamiento y almacenamiento en la nube. Finalmente se abordan las aplicaciones de visualización de datos.

Figura 7. Metodología utilizada en el desarrollo del proyecto.

La metodología propuesta para este trabajo consiste en los siguientes puntos.

1) Configuración del sistema IoV
2) Entorno de simulación.
3) Recolección de datos.
4) Filtrado de datos.
5) Análisis y procesamiento de datos.
6) Ciberseguridad.
7) Servicios de almacenamiento en la nube.
8) Aplicaciones.

El proceso seguido en el proyecto contempla inicialmente la configuración del entorno IoV. Dentro de la arquitectura, contemplamos un entorno de simulación para la extracción de datos. En este caso el simulador imita la red CAN bus de un vehículo. Como la cantidad de datos puede ser alta y en ocasiones no todos los datos son necesarios se realiza una etapa de seleccion de información que sea relevante.

Posteriormente, los datos seleccionados son procesados en los diferentes algoritmos que pueda necesitar el proyecto, por ejemplo, identificar casos delictivos sobre robos de vehículos que han sido reportados cerca de la posición del usuario.

Todos los datos de interés serán compartidos con el usuario, esto se realiza mediante la implementación de un servicio de almacenamiento en la nube. Sin embargo, derivado de la inseguridad que existe con respecto a los datos delicados en la red, la información compartida será cifrada antes de ser enviada y almacenada.

Finalmente, la información ya cifrada será interceptada por todos los elementos de interacción (app móvil, app web, programas internos) donde el usuario como los dispositivos externos serán capaces de visualizar de manera clara toda la información.

La descripción anterior es un resumen general sobre la metodología utilizada. Para comprender mejor, a continuación se dará una breve explicación sobre cada una de las etapas.

Configuración del sistema IoV

La etapa de configuración consiste en el armado de un sistema IoV. En esta etapa se deben considerar todas las funcionalidades que se quieren implementar, entre los que se encuentran la recopilación de datos, la ciberseguridad, los ambientes en la nube, los sistemas de procesamiento de datos y las aplicaciones que se realizan.

Entorno de simulación

El entorno de simulación permitirá imitar algunas funciones de un vehículo. Este hace uso de un paquete llamado CANsocket para simular el CAN bus de un automóvil. Dicho paquete es compatible con sistemas operativos basados en Linux y además es de acceso libre. La interfaz que se utiliza está desarrollada en python y además puede operar con la librería CAN del paquete CANsocket para leer en tiempo real los datos que circulan por el simulador.

Recolección de datos

La etapa de recolección de datos consiste en implementar scripts que se encargan de recopilar información sobre el vehículo y su entorno. En esta etapa se simulan diferentes funciones de un vehículo, los cuales generan datos que pueden ser recopilados en el simulador y posteriormente usarlos en otras actividades. Por ejemplo, se simula si el vehículo tiene los faros encendido o apagados. Dichos datos serán recopilados y procesados en las siguientes etapas. También se contemplan datos relacionados con la comunicación V2V y V2I, para saber si un vehículo se encuentra relativamente cerca de nosotros o cual es el estado del semáforo.

Filtrado de datos

La etapa de filtrado de datos permite seleccionar e identificar el tipo de dato que se obtiene durante el funcionamiento de un vehículo. Esto implica identificar qué datos se quieren procesar y cuáles no. Para lograr esto, se hace uso de un identificador Id que viene integrado en los mensajes CAN bus. El propósito del identificador es dar un nombre o una dirección única a la computadora automotriz que queremos analizar. Por ejemplo, existen una Id la cual identifica a la computadora que regula el estado de los faros.

Con ello sabremos qué mensajes son los que contienen esta información y así utilizarlos en las actividades vinculadas a estos datos de interés.

Análisis y procesamiento de datos

La etapa de análisis consiste en implementar algoritmos que procesan datos y generan algún resultado. Por ejemplo, se pueden utilizar algoritmos que permitan hallar sucesos que acontecieron cerca de nuestra ubicación. Ejemplo de estos son los algoritmos de vecinos cercanos o nearest neighbors en inglés.

Seguridad de los datos

La etapa de seguridad consiste en la implementación de algoritmos de cifrado de datos para dar protección a la información que queremos compartir en un entorno IoV. El propósito de esta etapa es propiciar que la información sólo sea comprendida e interpretada por aquellas entidades adecuadas, en especial, al compartir información en entornos públicos.

Servicios de almacenamiento en la nube

La etapa de implementación de servicios de almacenamiento consiste en desarrollar una serie de programas que nos brinden acceso a servicios en la nube en los cuales podamos almacenar información. El objetivo es que dicha información esté disponible en cualquier momento que se requiera. Para lograr esta actividad, se desarrollaron scripts en Python los cuales se encargaran de subir datos a la nube.

Aplicaciones

La etapa de aplicaciones corresponde con la implementación de aplicaciones que servirán como interfaz para que los usuarios puedan interactuar con la información. En esta instancia se desarrolló una aplicación móvil en la cual, los usuarios tendrán una cuenta personalizada donde observan algunos datos sobre su vehículo. Esta información contempla los niveles de la gasolina, el estado de los seguros, el estado de las ventanas (cerradas o abiertas), el estado de los faros (encendidos o apagados), entre otros.

4.3. **Implementación**

El presente trabajo tiene como objetivo implementar un sistema de cifrado de datos basado en criptografía para compartir información de manera segura en un ambiente de Internet de los vehículos. Dicho ambiente tiene su origen en los sistemas IoT en cual pretenden dar facilidad de monitoreo y control de cualquier sistema o aparato electrónico a través de algún dispositivo como una computadora, una laptop, un teléfono celular, etc. Para el caso de los entornos IoV la idea es similar, es decir, poder monitorear o manipular sistemas de un vehículo con la ayuda de algún dispositivo de manera remota.

Para comprender de mejor manera, podemos interpretar a los sistemas IOV como un sistema compuesto de sensores y actuadores que son capaces de obtener y procesar datos de diferente índole. Estos datos varían desde la ubicación de la unidad, hasta los datos internos sobre el estado en el que se encuentra un vehículo como la apertura y cierre de puertas, la proximidad con otros vehículos y otros datos como las señales de tránsito, el estado del semáforo, la proximidad con algunos peatones, entre otros. Además, gracias a la dependencia que tienen los entornos IoV a los servicios de internet, existen riesgos de seguridad que atentan en contra de la seguridad de la información de los vehículos como a la seguridad de sus ocupantes. Todos los datos generados pueden ser utilizados con diferentes propósitos y realizar alguna acción.

Pero, ¿Cómo se obtienen todos estos datos? Un vehículo moderno está constituido principalmente por varios sistemas como: el sistema de la transmisión, el módulo del motor, el sistema de dirección, el sistema de frenado, el sistema de infoentretenimiento, etc. Cada uno de estos sistemas están compuestos por un conjunto de sensores y actuadores los cuales se encuentran gobernados por una computadora central. Al final de todo, cada uno de los sensores, actuadores, computadoras y protocolos de comunicación constituyen una red vehicular.

En un vehículo moderno de gama media, el número de computadoras rebasan las 50 unidades y cada una de ellas se comunican entre sí. La forma más común para mantener a las computadoras conectadas es mediante un protocolo de comunicación. En el caso de los vehículos, el protocolo más conocido es el CAN bus.

La forma en que se comunican los sistemas internos de un vehículo es mediante el intercambio de mensajes a través del protocolo CAN Bus. Cada mensaje intercambiado tiene un destinatario específico, ya que las computadoras sólo procesarán aquellos msm que les sean de interés. Los mensajes poseen una estructura predeterminada que consiste en una marca de tiempo, un identificador ID, una trama de datos, etc. En realidad, existen más datos como un medidor del tamaño de la trama de datos, indicador de prioridad, etc. Sin embargo, los más utilizados en los análisis son los mencionados anteriormente.

Ejemplo.

0.01340000 016 08 00 01 03 00 00 00 00 00

tiempo ID tamaño trama

Lo podemos observar, existen una gran cantidad de datos que circulan a cada instante. De hecho, se considera que gracias a la implementación de nuevas tecnologías especiales para los vehículos inteligentes y autónomos, la cantidad de datos que se pueden recopilar durante cierto tiempo de funcionamiento pueden alcanzar los terabytes.

Consideraciones

Para las tecnologías IoV, los diferentes sistemas de comunicación entre el vehículo y su entorno como la comunicación V2X (vehículo a todo), V2V (vehículo a vehículo), V2I (vehículo a infraestructura) o V2P (vehículo a peatón) otorgan más cantidad de datos. Algunos ejemplos de estos datos consisten en recopilar información sobre el estado del semáforo para que el propietario del vehículo pueda observar dicha información en una pantalla incorporada en el interior del vehículo. Incluso ante situaciones más complejas permitirá al automóvil actuar por sí solo.

Para los sistemas autónomos esta característica toma más relevancia, ya que dependiendo del tipo de información recibida por el propio vehículo como del entorno, se logra la conducción autónoma. El problema con este tipo de sistemas es su carencia de herramientas de ciberseguridad que protejan los datos, especialmente con las nuevas tecnologías de comunicación que mantienen conectados el vehículo con el entorno.

¿Por qué es importante lo anterior? Esto servirá de partida para comprender cómo se comunican los vehículos, qué elementos intervienen y cómo son estructurados los mensajes que son intercambiados. De esta manera seremos capaces de identificar algunos puntos importantes que deben ser tomados en cuenta para el desarrollo del proyecto. Dicho lo anterior, si queremos desarrollar un sistema de ciberseguridad basado en criptografía u otros sistemas como podría ser blockchain, hay que tomar en cuenta que algunos aspectos pueden perjudicar su correcta implementación.

Algunos algoritmos encargados de monitorear sistemas como en el caso de la comunicación V2I (vehículo a infraestructura) o V2X (vehículo a todo), el sistema tendrá mayor flexibilidad para manipular datos. Sin embargo, en sistemas más complejos y delicados como la comunicación V2V (vehículo a vehículo), resultó ser una tecnología bastante especial pues puede verse comprometida por diferentes factores.

En el caso de la comunicación vehículo a vehículo, debemos tomar en cuenta la velocidad de transmisión de los datos la cual debe ser considerablemente rápida para que los sistemas involucrados se activen rápidamente en caso de ser necesario. Por ejemplo, activar los frenos rápidamente si se detecta algún accidente más adelante. Al implementar sistemas criptográficos en este tipo de comunicación se observa que los tiempos de ejecución de los mismos pueden ser considerablemente altos. Otro aspecto importante puede ser la latencia, pues se requiere que no existan demoras, retrasos o reacciones tardías durante la transmisión de información.

También tenemos algunas cuestiones sobre el almacenamiento, ya que al trabajar con datos de un vehículo, se considera que el flujo de dicha información puede alcanzar los terabytes de datos. Para un sistema blockchain la cantidad de datos puede ser demasiada alta, lo que significa que se necesitará mucho almacenamiento a largo plazo. La Tabla 10 describe de mejor manera algunos aspectos importantes sobre el uso de blockchain y de criptografía aplicada en los sistemas de Internet de los vehículos.

4.4. **Descripción del sistema propuesto**

Son numerosas las aplicaciones que se pueden desarrollar con toda la información obtenida en un vehículo. Sin embargo, también debemos tener en cuenta cuáles son las limitaciones que se tienen para el desarrollo de un proyecto.

El sistema propuesto en este trabajo consiste en la implementación de aplicaciones del entorno del internet de los vehículos. Dichas aplicaciones contemplarán entornos de ejecución para sistemas de comunicación interna del vehículo y datos en las comunicaciones V2I, V2E y V2V.

Se desarrollará una interfaz de simulación del protocolo CAN Bus para imitar procesos de un automóvil real. Los datos obtenidos serán protegidos mediante algoritmos de cifrado y almacenados en la nube para su uso en las diferentes aplicaciones. La Figura 8 describe la idea general del proyecto.

Figura 8. Idea general de un sistema IoV

Lo que se busca en este proyecto de forma general es realizar un sistema que sea capaz de obtener datos de un vehículo, subir la información a la nube y compartirla de forma segura con el usuario. Además se apoyará de una aplicación móvil y un programa interno dentro del vehículo para que el usuario y el propio vehículo interactúen con los datos.

El problema que se ha contemplado en estos sistemas (IoV), es que los datos no se encuentran protegidos. Derivado de esto se pretende desarrollar un programa que pueda obtener datos del vehículo, cifrarlos y subirlos a la nube. Los datos sólo llegarán y serán interpretados por aquellas entidades autorizadas. De esta manera se busca lograr los servicios de confidencialidad y autenticación de los datos que operan en los entornos de IoV. En la Figura 9 se muestra cómo puede ser implementado un algoritmo criptográfico en un sistema de internet de los vehículos.

Figura 9. Sistema IoV con cifrado de datos

4.5. **Configuración del sistema IOV**

Parte del desarrollo de un sistema IoV es contemplar la estructura que este tendrá. En la literatura existen diferentes configuraciones que han sido propuestos por varios autores. De hecho, en el estado del arte del presente trabajo se observan algunos ejemplos simples que contempla 3 fases o capas hasta sistemas más complejos con más de 6 capas. En estas estructuras cada una de las capas tienen asignada una tarea específica y de alguna manera se encuentran correlacionadas entre sí.

El sistema propuesto en este trabajo consiste en una arquitectura de 5 capas: la capa de monitoreo, la capa de procesamiento, la capa de ciberseguridad, la capa de servicios en la nube y la capa de aplicaciones. En la Figura 10 se muestra la configuración del sistema IoV que fue utilizada.

Figura 10. Configuración del sistema IoV utilizado

Capa de monitoreo: Es la encargada de recopilar datos de cada uno de los sistemas que conforman a un auto. En esta capa se integrarán tanto los datos internos del auto como los datos del entorno.

Capa de procesamiento: Se encarga de filtrar, analizar y procesar los datos obtenidos.

Capa de ciberseguridad: Tiene la tarea de proteger los datos que serán intercambiados en ambientes públicos de los sistemas IoV.

Capa de servicios en la nube: Es la encargada de gestionar y filtrar los datos que serán enviados, almacenados y recolectados de la nube.

Capa de aplicaciones: Es la encargada de aprovechar la información obtenida para generar aplicaciones. Esta capa permitirá a los usuarios como a otros vehículos, visualizar e interactuar con la información recopilada.

4.6. **Equipo y herramientas utilizadas**

En el desarrollo de aplicaciones IoT e IoV generalmente utilizan dispositivos que son capaces de obtener, procesar y analizar información. En estos ambientes suelen utilizarse placas de desarrollo Arduino y Raspberry pues son muy amigables y fáciles de utilizar. En este caso, se optó por utilizar algunas placas Raspberry (Figura 11).

Figura 11. Raspberry

El lenguaje de programación utilizado fue Python (Figura 12). Dicho lenguaje es muy flexible, ya que existen muchas librerías que permiten realizar diferentes tareas. Estas tareas pueden ser tan complejas como se requiera. De hecho hay librerías tan simples que realizan operaciones matemáticas como sumas y restas hasta complejos algoritmos como pueden ser las redes neuronales.

Figura 12. Python

Para este trabajo, las librerías utilizadas en los experimentos se muestran a continuación.

- Can tools
- Firebase
- Cripto

Para la implementación de servicios en la nube se utilizó Firebase (Figura 13). Este servicio es proporcionado por Google y es de acceso gratuito. En esta plataforma podemos enlazar y compartir datos entre aplicaciones que fueron desarrolladas en diferentes entornos como las páginas web o las aplicaciones móviles. Dentro de las herramientas que proporciona Firebase, encontramos las siguientes.

- Authentication
- Database

Figura 13. Firebase

Para la implementación de una aplicación móvil se contempló utilizar Android Studio (Figura 14). En esta aplicación se accedió internamente a los datos almacenados en la nube para procesar y posteriormente visualizarlos en diferentes pantallas de la aplicación.

Figura 14. Android Studio

Finalmente, se requirió de Python para crear programas que tienen la tarea de acceder a los datos almacenados en Firebase y generar una acción específica. Estos programas se ejecutan internamente y permitirán procesar datos que proceden de fuentes externas en las diferentes formas de comunicación (V2I, V2E, V2V). Esta fase se realiza entre 2 Raspberry que simulan una comunicación entre 2 vehículos reales.

4.7. **Entorno de simulación**

En esta parte del trabajo se utilizó un entorno de simulación llamado SocketCan. Dicho entorno es de código abierto y permite simular el protocolo de comunicación CAN bus de un vehículo por el cual circula información. Los datos que circulan por el simulador consisten en mensajes que se apegan al formato de un msm CAN real (un identificador ID y un frame de datos). El ID representa un código de identificación que posee una computadora específica que está gobernando algún sistema. De hecho, cada computadora se encuentra identificada con un ID diferente el cual es utilizado por las demás computadoras para saber qué mensajes pueden procesar y cuáles no. En la Figura 15 se muestra la interfaz que simula el CAN bus de un vehículo. La Figura 16 muestra el flujo de datos en el simulador.

Figura 15. Interfaz del simulador de un vehículo

Figura 16. Ventana de flujo de datos en el simulador

4.8. **Implementación de servicios de almacenamiento en la nube**

Los experimentos realizados en esta etapa consisten en implementar un servicio de almacenamiento de datos en la nube. Actualmente, en el mercado existen muchas plataformas con diferentes características y requerimientos, sin embargo, la plataforma seleccionada para utilizar un servicio de almacenamiento fue Firebase. Esta plataforma es muy intuitiva y amigable con el usuario, además, es de libre acceso. Dentro de sus servicios permite el almacenamiento de información en tiempo real, el almacenamiento de imágenes, servicios de autenticación, etc. En la Figura 17 se muestran algunas de las herramientas que ofrece Firebase.

Figura 17. Herramientas disponibles en Firebase

4.9. **Experimentos**

En este apartado se describen algunos experimentos realizados donde se utilizan sistemas de ciberseguridad que pueden ser aplicados en los entornos IOV. En este proyecto se contempla utilizar algoritmos de cifrado

4.11. **Implementación de algoritmos criptográficos**

Los experimentos realizados en esta parte corresponden con el uso de algoritmos criptográficos. Para iniciar debemos comprender algunos aspectos importantes sobre la criptografía, en primer lugar, tenemos 2 tipos de criptografía, la simétrica y la asimétrica.

Criptografía simétrica: Utiliza una sola llave para cifrar y descifrar los datos.

Criptografía asimétrica: Requiere de una llave pública para cifrar y una privada para descifrar o viceversa.

En la Figura 19 se describe el proceso de cifrado/descifrado de un algoritmo de criptográfico simétrico. Para el caso de la criptografía simétrica tenemos algunos algoritmos como DES y AES. En la Figura 20 se describe el proceso de cifrado del algoritmo criptográfico asimétrico. Para la criptografía asimétrica se tienen algunos algoritmos como lo es RSA.w Igualmente existe algún algoritmo híbrido básicamente consiste en la unión de un sistema simétrico con uno asimétrico.

Figura 19. Proceso de cifrado/descifrado del algoritmo criptográfico simétrico

Figura 20. Proceso de cifrado/descifrado del algoritmo criptográfico asimétrico

En los experimentos se contempló ver el comportamiento de cada uno de los algoritmos. El objetivo era encontrar el que mejor se adapte con base a los resultados y a sus características particulares. Para su desarrollo se realizaron algunos scripts en Python que se encargan de obtener, procesar y cifrar datos con sus llaves correspondientes. Una sola llave es utilizada para el cifrado simétrico y un par de llaves pública/privada para el cifrado asimétrico. Las llaves generadas son compartidas para que el receptor realice el proceso de descifrado. De este modo, el usuario como el sistema será capaz de interpretar y comprender la información que obtuvo.

Para comenzar crearemos un programa Script que nos permita acceder al simulador can bus y leer los mensajes que circulan por él. La librería “Can” posee muchas herramientas que nos permiten realizar este tipo de tareas. Para utilizar la librería debemos especificar el tipo de protocolo utilizado seguido de la función “Recv()”. Con estos elementos seremos capaces de leer e interpretar los mensajes que circulan por dicho protocolo. La Figura 21 muestra un extracto del código necesario para leer los datos que circulan por el simulador.

Figura 21. Código requerido para leer mensajes en el simulador CAN bus

Una vez que tenemos acceso a los datos que circulan por el simulador, proseguimos con el agrupamiento de los datos que queremos utilizar. Es decir, filtraremos la información que nos es de más utilidad.

4.11.1. **Etapa de generación de llaves**

En la etapa de ciberseguridad se utilizaron los algoritmos respectivos para proteger los datos. Para que estos algoritmos funcionen adecuadamente, en primera instancia hay que generar las llaves adecuadas. Existe un librería llamada PBKDF2 la cual nos permite generar claves seguras y con un formato específico. De esta manera podemos crear las llaves de 128, 192 y 256 bits que son requeridas en el cifrado AES. Para el caso del algoritmo DES, la llave generada es de 56 bits. La Figura 22 muestra las llaves que fueron generadas con la librería PBKDF2.

Figura 22. Generación de llaves requeridas para cifrar datos

Uno de los factores más importante fue seleccionar el nivel de seguridad en los algoritmos. El algoritmo de cifrado DES solo utiliza llaves de cifrado de 56 bits, lo cual lo hace vulnerable a una gran cantidad de ataques debido al poder de procesamiento de la tecnología moderna. Hoy en día, el cifrado DES se considera obsoleto debido a su baja seguridad. De hecho, existen experimentos en los cuales se logra romper un mensaje cifrado con DES en solo 22 horas.

Por otro lado, AES ha mostrado mejores características de seguridad gracias a la complejidad de sus llaves. Un algoritmo de cifrado AES posee llaves con mayor longitud lo que aumenta la cantidad de combinaciones posibles para generar una llave. De este modo, también aumenta la complejidad en caso de ser atacados. Para el algoritmo de cifrado AES las longitudes de llaves utilizadas son de 128, 192 y 256 bits. ¿Pero qué tan seguras son? En primera instancia, para poder atacar un sistema mediante fuerza bruta se

requiere de un poder de cómputo bastante alto. Además, la cantidad de intentos que se requieren para dar con una llave adecuada crece considerablemente entre mayor es la longitud de la llave.

En la Figura 23 se observan algunos ejemplos relacionados con la generación de llaves. En ella podemos distinguir que la longitud de la cadena aumenta entre mayor sea el número de bits utilizados y por lo tanto, también aumenta su fuerza. Cabe mencionar que AES solo acepta las últimas 3 llaves.

Figura 23. Ejemplos de llaves generadas en los experimentos

Otra manera de ver la complejidad de las llaves es mediante la cantidad de combinaciones posibles que se pueden generar para las llaves. En el caso de las llaves de 128 bits se requieren de 2^128 combinaciones posibles para generar una llave, con las llaves de 192 se requieren de 2^192 combinaciones y finalmente para una llave de 256 bits requerimos de 2^256 combinaciones posibles. La Tabla 13 muestra la cantidad de combinaciones necesarias para diferentes longitudes de llaves. La Figura 24 muestra el tiempo requerido para generar las llaves

Tabla 12. Combinaciones requeridas para generar llaves de cifrado AES

Figura 24. Tiempo de generación de llaves AES

De lo anterior se concluye que el uso de llaves mayores a los 128 bits es adecuado para garantizar una fuerte seguridad. Aunque estas llaves ya son relativamente estables, usar llaves mayores no representa un problema ya que los tiempos de generación son casi iguales. Además, el tamaño de la llave generada es mucho mayor y en consecuencia aumenta la fuerza de descifrado durante un ataque. Incluso teniendo la capacidad de cómputo adecuada, el tiempo de cifrado y descifrado por fuerza bruta tomaría bastante tiempo. Esto ya no es una característica adecuada si consideramos que el algoritmo almacena, genera llaves y cifra datos entre los 2 y 3 segundos. Por lo anterior, se utilizaron llaves de 256 bits durante los experimentos debido a sus características y ventajas.

En el caso del cifrado RSA existen otro conjunto de llaves que son utilizados frecuentemente en dicho algoritmo. La Tabla 14 muestra las llaves que son más utilizadas. En ella se observa que las llaves utilizadas con mayor frecuencia van desde un tamaño mínimo de 512 bits hasta llaves de tamaño máximo de 4096 bits. En la Figura 25 se muestra el tiempo requerido para generar estas llaves.

Tabla 13. Longitud de llaves utilizadas en el cifrado RSA

Figura 25. Tiempos de generación de llaves RSA

Derivado de lo anterior, se concluye que utilizar llaves mayores a los 4096 requiere mayor cantidad de tiempo y también mayor capacidad de cómputo. Esto refleja la complejidad que se requiere para generar una clave de mayor longitud. De lo anterior se observa que las llaves de 2048 bits son muy adecuadas ya que cuentan con una alta fuerza de cifrado, además de un tiempo moderado de generación de llave.

4.11.2. **Etapa de cifrado**

Una vez obtenidas las llaves correspondientes, comenzamos con el proceso de cifrado de los datos. Para ello utilizamos una función encargada de emplear los algoritmos de cifrado y junto con la llave generada en el paso anterior ciframos los datos que queremos proteger. El proceso descrito anteriormente fue realizado para probar los algoritmos de cifrado DES, AES y RSA. La Figura 26, Figura 27 y Figura 28 muestra un extracto del código utilizado para cifrar los datos. En ella se observa que se requiere de la información que queremos cifrar seguido de las llaves que generamos anteriormente para proceder con el cifrado, de lo contrario existirán errores.

Figura 26. Cifrado de datos con el algoritmo DES

Figura 27. Cifrado de datos con el algoritmo AES

Figura 28. Cifrado de datos con el algoritmo RSA

4.11.3. **Etapa de almacenamiento**

En cada caso se utilizó un algoritmo de cifrado completamente diferente, pero el proceso de almacenamiento en la nube era el mismo para los 3 casos. La manera de almacenar los datos era mediante la función ”data_ref.set()” que permite estructurar los datos y almacenar la información previamente establecida en Firebase. Las siguientes imágenes muestran la implementación de los algoritmos utilizados en el proyecto. La Figura 29 muestra un extracto del programa necesario para almacenar los datos cifrados con el algoritmo AES en la nube. La Figura ? muestra el extracto utilizado para almacenar datos cifrados con RSA.

Figura 29. Programa utilizado para almacenar los datos cifrados en Firebase

De igual manera, las siguientes imágenes muestran datos que fueron almacenados en Firebase. La Figura 30 representa a los datos cifrados con AES que fueron almacenados. La Figura 31 representa a los datos cifrados con RSA que fueron almacenados en Firebase.

Figura 30. Datos cifrados con AES y almacenados en Firebase

Figura 31. Datos cifrados con RSA y almacenados en Firebase

Como se puede observar, los resultados arrojados en cada experimento variaron de acuerdo al algoritmo utilizado. En los algoritmos AES y DES obtenemos cadenas de texto de cifrado con un tamaño moderado. Para el caso del algoritmo RSA las cadenas resultantes eran más largas y complejas. En los 3 casos el texto es completamente incomprensible para una persona. La única manera de comprender el contenido del texto es utilizando una llave adecuada que permita descifrar la información.

Existen muchos factores de gran importancia que son necesarios para implementar sistemas IoV, especialmente para gestionar datos que provienen o que están destinados a funciones críticas de los vehículos. A continuación en la Tabla 14 se muestran los resultados obtenidos por los algoritmos que fueron probados.

Tabla 14. Resultados obtenidos en los experimentos

Se concluye que AES y RSA muestran mejores características que DES. Estos cuentan con mejores niveles de seguridad, mayor complejidad y mejores tiempos de ejecución independientemente de que en la actualidad el cifrado DES se considera obsoleto. Por otra parte, aunque los sistemas de cifrado RSA tienen mayores niveles de seguridad, su tiempo de ejecución se ve perjudicado. Al observar los algoritmos se notó que el tiempo de generación de la llave en el algoritmo RSA toma bastante tiempo, mientras que el proceso de cifrado no demora mucho tiempo. En consecuencia, se optó por generar llaves por periodos de tiempo específicos para disminuir el tiempo de generación. De esta manera, la velocidad de cifrado se hizo más rápido.

4.12. **Sistema de cifrado híbrido**

Los experimentos anteriores mostraron resultados aceptables tanto para los algoritmos de cifrado simétrico como para los de cifrado asimétrico. Sin embargo, utilizar cifrado simétrico tiene desventajas a largo plazo. El problema es que si un atacante logra obtener la llave, este será capaz de descifrar los datos. En cambio, si utilizamos un algoritmo que utilice lo mejor del cifrado simétrico como asimétrico, obtendremos un algoritmo más seguro y robusto. A este tipo de programas se le conoce como algoritmo de cifrado híbrido. Dicho programa muestra gran flexibilidad y complejidad al cifrar 2 veces un mismo mensaje mediante una llave simétrica y un conjunto de llaves (la llave pública y la llave privada). La Figura 32 muestra el proceso de cifrado en un algoritmo híbrido.

En este algoritmo, el proceso contempla dos rondas de cifrado. Los algoritmos de cifrado que se utilizan pueden variar, por ejemplo, podemos utilizar el cifrado AES en primera instancia para obtener un primer mensaje cifrado. El mensaje resultante será proporcionado a la siguiente fase donde se realizará el segundo cifrado. Para la segunda etapa de cifrado existen algoritmos asimétricos como el cifrado RSA.

Para llevar a cabo ambos procesos, primero debemos empezar con la generación de la llave simétrica y las llaves asimétricas (una llave pública y otra privada) que serán utilizadas para proteger los datos. La llave simétrica servirá tanto para cifrar como para descifrar información, mientras tanto, la llave pública solo será utilizada para cifrar datos. La tarea de la llave privada será descifrar el mensaje para saber su contenido. Una vez que obtenemos el texto cifrado se procede a intercambiar la llave simétrica y el mensaje modificado para que el receptor pueda descifrar el mensaje y utilizar la información a su criterio.

Figura 32. Proceso de cifrado en un algoritmo híbrido

4.13. **Implementación de un sistema IoV con cifrado híbrido**

La capa de ciberseguridad será la encargada de implementar el algoritmo de cifrado híbrido. Los experimentos realizados en esta sección consisten en utilizar el algoritmo AES y el algoritmo RSA para obtener un sistema de cifrado híbrido. El proceso seguido en este algoritmo comprende los siguientes puntos.

1) Obtener los datos.
2) Cifrar los datos con AES.
3) Volver a cifrar los datos con RSA.
4) Almacenar los datos en la nube.

Las características tomadas en cuenta para desarrollar este algoritmo consiste en el uso de llaves de 256 bits de longitud para él algoritmo de cifrado AES. La longitud de las llaves RSA seleccionadas fueron de 2046 bits de longitud. El nivel de seguridad que tiene el algoritmo es alto, considerando que la complejidad para quebrantar llaves de 256 bits requiere de más de 2^256 combinaciones posibles para dar con la llave adecuada. Incluso, el cifrado RSA solo aumenta aún más la complejidad ya que la llave privada se mantendrá oculta en todo momento.

De lo anterior hay que tomar en cuenta que para realizar un ataque de fuerza bruta y obtener el mensaje original, se necesitará generar una llave AES y posteriormente una llave privada. Sabemos que los tiempos de cifrado e intercambio de información con la nube se realizan en intervalos de tiempo comprendidos entre los 2 y 3 segundos aproximadamente. Aunado a esto, tenemos que en cada instancia se generan diferentes llaves aleatorias y solo se cuenta con 2 segundos para obtener las diferentes llaves y quebrantar el mensaje. Prácticamente sería imposible obtener la información original.

La Figura 33 muestra un extracto del programa utilizado para realizar el cifrado híbrido, es decir, el cifrado AES seguido del cifrado RSA.

Figura 33. Datos cifrados con el algoritmo híbrido

Finalmente, estructuramos los datos en la función adecuada para almacenar los datos en la nube. La Figura 34 muestra la información que fue almacenada exitosamente en Firebase.

Figura 34. Datos almacenados en Firebase que fueron cifrados con el algoritmo híbrido

Una vez que los algoritmos de cifrado fueron desarrollados y ejecutados exitosamente, y que además los datos ya fueron almacenados en la nube, se comenzarán a implementar las diferentes aplicaciones que aprovechen esta información. Estas aplicaciones tendrán la tarea de generar un entorno en el que los usuarios u otras entidades como los vehículos puedan interactuar con la información. Las aplicaciones contempladas consisten en programas internos que se encargan de intercambiar información entre el vehículo y su entorno (V2E), entre el vehículo y otros vehículos (V2V) y entre el vehículo y la infraestructura (V2I).

Además, se contempla desarrollar una aplicación móvil que permitirá rastrear el vehículo en cualquier momento. Dicha aplicación también permitirá observar el estado en el que se encuentra el vehículo, es decir, cuánta gasolina tiene, si las puertas fueron cerradas correctamente, si las ventanas están bien cerradas, entre otras cosas.

4.14. **Implementación de programa interno para la comunicación V2X**

Un factor muy importante en los sistemas IoV es el intercambio de datos entre vehículos. Estos han tomado más fuerza gracias a los vehículos autónomos, ya que estos se apoyan de una gran cantidad de sensores que recopilan información del entorno. Prácticamente los vehículos autónomos intercambian y reciben información del entorno y otros vehículos para saber su ubicación, su cercanía, su velocidad. Basándose en la información recopilada, el automóvil podrá tomar una decisión adecuada al momento de ejecutar alguna acción específica. Un claro ejemplo podría ser el adelantamiento a algún automóvil sabiendo que en la vía adyacente no hay alguna unidad cercana que suponga algún riesgo.

Para esta sección la comunicación V2V requiere la intervención de un conjunto de vehículos que se encuentren comunicándose entre sí. Para este caso se utilizaron 2 dispositivos Raspberry los cuales simularán dos vehículos que se están comunicando. Estos contendrán un programa interno que recopila información interna y externa del vehículo. Además se encargan de cifrar los datos y los intercambian de forma segura en un ambiente IoV. La Figura 35 muestra un extracto del programa generado en Python para gestionar la comunicación del vehículo con su entorno, lo que implica la comunicación V2V (cercanía con otros autos), V2I (estado de los semáforos, señales de tránsito) y V2E (ubicación, presencia de peatones, presencia de obstáculos, zona de accidente).

Figura 35. Programa que gestiona información relacionada con la comunicación con el entorno

4.15. **Implementación y desarrollo de una aplicación Android**

Las aplicaciones móviles hoy en día han tomado un gran auge en la vida diaria de las personas. En muchos casos, estas aplicaciones nos permiten realizar muchas tareas. Algunos ejemplos consisten en el desarrollo de aplicaciones enfocadas en los sistemas IoT enfocados en los sistemas de domótica. Estos permiten supervisar muchas funciones de las viviendas inteligentes.

El objetivo de esta aplicación será ofrecer un entorno donde los usuarios puedan visualizar diferentes aspectos del vehículo como por ejemplo la localización geográfica de la unidad o el estado en el que se encuentran algunas partes del vehículo como las puertas, las ventanas, los seguros, la cajuela, los faros, entre otros.

El usuario también tendrá un perfil personalizado donde solo verá datos relacionados con su propio vehículo. Para ello se usarán los servicios de autenticación de Firebase para poder almacenar diferentes usuarios. Cada usuario tendrá una cuenta propia que estará identificada mediante un correo y una contraseña. La aplicación tendrá incorporada una ventana donde podemos ingresar esta información y generar un usuario. La Figura 36 muestra la ventana utilizada para iniciar sesión en la cuenta del usuario así como la pantalla encargada de generar un nuevo usuario. La Figura 37 muestra al usuario generado correctamente en la base de datos de Firebase.

Figura 36. Ventana de Inicio de sesión y creación de usuario

Figura 37. Usuario almacenado en la base de datos de Firebase

Posteriormente, la aplicación accedera en segundo plano a las bases de datos de Firebase para obtener datos de interés. Estos datos serán descifrados y distribuidos en las diferentes pantallas que tendrá la aplicación. La primera ventana contiene datos personales sobre el usuario (Figura 38). Los datos que se contemplan son el nombre del usuario, su correo electrónico y el tipo de vehículo que maneja.

Figura 38. Ventana principal de la aplicación

La Figura 39 muestra la pantalla que es utilizada para mostrar la ubicación geográfica de la unidad. Para ello se emplea Open Street Maps que permite implementar mapas donde podemos visualizar de forma exacta la ubicación del auto.

Figura 39. Ventana de monitor de la ubicación de la unidad

La pantalla de la Figura 40 se utilizará para observar algunos aspectos del automóvil. Estos contemplan el estado de las puertas, las ventanas y la cajuela de la unidad. Se observará si estas partes fueron cerradas correctamente o si se encuentran abiertas.

Figura 40. Ventana de monitores de las puertas del automóvil

La tercera pantalla de la Figura 41 contempla el monitoreo sobre los niveles de combustible del vehículo.

Figura 41. Ventana de monitorea de los niveles de combustible del automóvil sawqew

Capítulo 5. Conclusiones y trabajo a futuro

5.1. **Conclusiones**

Los sistemas IoV han tenido un gran auge con el paso del tiempo. De manera similar a como ocurre con los sistemas IoT, estos carecen de sistemas de seguridad que den respaldo a los datos. En consecuencia, se observa que es necesario implementar algún sistemas de ciberseguridad que proteja los datos.

Los algoritmos de cifrado son una gran opción para proteger los datos y son flexibles para implementar aplicaciones. Del mismo modo, se observó que los algoritmos de cifrado simétrico pueden ser implementados de manera satisfactoria en una aplicación IoV ya que los tiempos de ejecución de los algoritmos son relativamente moderados para compartir información.

Para el caso de la comunicación V2V en los sistemas IoV, es necesario acotar el uso de estos programas, pues en sistemas críticos su uso se ve encarecido. Un ejemplo de ello es el intercambio de información durante algún choque. En esta situación se busca avisar a los vehículos cercanos sobre la situación. En estos casos, los tiempos de acción y reacción deben ser demasiado rápidos. En dichos casos la criptografía se ve limitada.

Por el contrario, si lo que se busca en la comunicación es informar sobre el estado del semáforo en una calle dada, los algoritmos pueden ser usados perfectamente ya que la situación es más flexible.

Los algoritmos de cifrado asimétrico son una versión más compleja y segura, sin embargo suelen requerir de mayor poder de cómputo así como de tiempo. El tiempo para las aplicaciones de este estilo es un factor muy importante que se tiene que contemplar.

Al realizar los experimentos, se observó que los algoritmos tardan en generar las llaves, lo que hace más lento la ejecución del programa. Una alternativa que se planteó fue la generación de llaves en intervalos de tiempo. En estos casos, el cifrado asimétrico se vuelve viable.

Además, la llave pública que fue generada en el cifrado asimétrico será compartida para que los demás puedan cifrar los datos que se requieren. Solo el usuario o las entidades correctas que poseen la llave privada podrá descifrar la información y realizar alguna acción.

Se observó que el uso de llaves adecuadas para el cifrado AES es de 256 bits. Para las llaves asimétricas (la pública y la privada) se usarán llaves de 2048 bits. Además las llaves RSA muestran mayor robustez y por lo tanto son más seguras.

Por último, realizar un algoritmo que fusione ambos tipos de cifrado es una buena implementación y mucho más segura. Esto se debe a que la persona que tiene la llave adecuada podrá descifrar los datos independientemente si un hacker logra obtener las otras llaves (la simétrica o la pública).

5.2. **Trabajo a futuro**

El trabajo futuro consiste en implementar más funciones de monitoreo y más variedad de datos que puedan ser intercambiados en las diferentes formas de comunicación del vehículo (V2X, V2I, V2E. y V2V).

Realizar un sistema que permita adquirir y procesar datos de un vehículo real.

Implementar el sistema propuesto en un caso de estudio real, como el seguimiento de una flotilla de unidades.

Referencias

1. General Motors de México. OnStar. https://www.onstar.com.mx/. Consultado en el 2024

2. Lo/Jack. https://lojack.com.mx/. Consultado en el 2024

3. Samzara. https://www.samsara.com/mx/pages/gps-tracking/. Consultado en el 2024

4. Foam Location. https://foam.space/. Consultado en el 2024

5. Dongdong Yuan & Yankai Wang. (2020). An Unmanned Vehicle Trajectory Tracking Method based on Improved Model-free Adaptive Control Algorithm. *2020 IEEE 9th Data Driven Control and Learning Systems Conference (DDCLS)*. IEEE.

6. Xiangdi Liu, Yunlong Dong & Zelin Deng. (2020). Deep Highway Multi-Camera Vehicle Re-ID with Tracking Context. 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). IEEE.

7. Taku Noguchi, Yu-Cheng Ting, Masami Yoshida & Alberto Gallegos Ramonet. (2020). Real-time Cooperative Vehicle Tracking in VANETs. 2020 29th International Conference on Computer Communications and Networks (ICCCN). IEEE.

8. Asep Najmurrokhman, Kusnandar, Ahmad Daelami, Udin Komarudin & Muhamad Ima. (2021). Design and Implementation of Vehicle Speed Recorder using GPS Tracker and Internet-of-Things Platform. 2021 International Conference on Artificial Intelligence and Computer Science Technology (ICAICST). IEEE.

9. Ning Li, Caixia Lu, Xuewei Yu, Xueyan Liu & Bo Su. (2021). Real-time 3D-Lidar, MMW Radar and GPS/IMU fusion based vehicle detection and tracking in unstructured environment. 2021 IEEE International Conference on Robotics and Automation (ICRA). IEEE.

10. Sumalatha Aradhya, Shashi Kumar, P Rudraradhya, S Thejaswini & A Soumya. (2021). Real Time Vehicle Tracking, Information Retrieval and Motion Analysis using Machine Learning. 2021 International Conference on Intelligent Technologies (CONIT). IEEE.

11. Kai Tian, Yun Li, Shanlin Sun & Biaohang Sun. (2022). Vehicle tracking from Bird-Eye view. 2022 IEEE 22nd International Conference on Communication Technology (ICCT). IEEE.

12. Ciyun Lin, Yue Wang, Bowen Gong & Hongchao Liu. (2023). Vehicle detection and tracking using low-channel roadside LiDAR. Measurement. Elsevier.

13. Zhanbo Sun, Zhihang Huang, Peng Hao, Xuegang (Jeff) Ban & Tianyu Huang. (2024). Batch-based vehicle tracking in smart cities: A Data fusion and information integration approach. Information Fusión. Elsevier.

14. Bo Yang, Mingyue Tang, Shaohui Chen, Gang Wang, Yan Tan & Bijun Li. (2020). A vehicle tracking algorithm combining detector and tracker. EURASIP Journal on Image and Video Processing. Springer.

15. Xiaoxu Liu, Wei Qi Yan & Nikola Kasabov.(2023). Moving vehicle tracking and scene understanding: A hybrid approach. Multimedia Tools and Applications. Springer.

16. Shumei Liu, Yao Yu, Wenjian Hu, Yuhuai Peng & Xiaolong Yang. (2020). Intelligent Vulnerability Analysis for Connectivity and Critical-Area Integrity in IoV. IEEE Access. IEEE.

17. Yousik Lee, Samuel Woo, Yunkeun Song, Jungho Lee & Dong Hoon Lee. (2020). Practical Vulnerability-Information-Sharing Architecture for Automotive Security-Risk Analysis. IEEE Access. IEEE.

18. Ahmed Abdullahi, Tooska Dargahi & Meisam Babaie. (2020). Vulnerability Assessment Of Vehicle To Infrastructure Communication: A Case Study Of Unmanned Ground Vehicle. 2020 IEEE Globecom Workshops (GC Wkshps). IEEE.

19. Manuel Mar, Julien Noel & J. Eric Dietz. (2021). Cyber-Physical Review of a Battery Electric Vehicle Power Train: Vulnerabilities and Challenges. 2021 IEEE PES Innovative Smart Grid Technologies Conference - Latin America (ISGT Latin America). IEEE.

20. Yinghui Wang, Bin Yu, Haiyang Yu, Lingyun Xiao, Haojie Ji & Yanan Zhao. (2022). Automotive Cybersecurity Vulnerability Assessment Using the Common Vulnerability Scoring System and Bayesian Network Model. IEEE Systems Journal. IEEE.

21. Shen S. Shiwen, Guo Z. Zhen, Liu T. Tianling, Bian C. Chenya, Ning Y. Yuqiao & Chen Y. Yang. (2023). Research and Analysis of Vulnerabilities in Intelligent Connected Vehicle Components. 2023 6th International Conference on Data Science and Information Technology (DSIT). IEEE.

22. Yujia Li, Yueyou Wang, Jue Wang, Hanbing Wu & Xianzhao Xia. (2023). Research on data security risk of intelligent and connected vehicles. 2023 International Conference on Mechatronics, IoT and Industrial Informatics (ICMIII). IEEE.

23. Yuvraj Singh, Somendra Singh, Palak Jain, Saumitra Chattopadhyay & Gagan Deep Singh. (2023). Security Vulnerability in the Automotive Sector with Modernization. 2023 IEEE 11th Region 10 Humanitarian Technology Conference (R10-HTC). IEEE.

24. Zaina Abuabed, Ahmad Alsadeh & Adel Taweel. (2023). STRIDE threat model-based framework for assessing the vulnerabilities of modern vehicles. Computers & Security. Elsevier.

25. Huimin Chen, Jiajia Liu, Jiadai Wang & Yijie Xun. (2023). Towards secure intra-vehicle communications in 5G advanced and beyond: Vulnerabilities, attacks and countermeasures. Vehicular Communications. Elsevier.

26. Gianpiero Costantino & Ilaria Matteucci. (2023). Reversing Kia Motors Head Unit to discover and exploit software vulnerabilities. Journal of Computer Virology and Hacking Techniques. Springer.

27. R. Amala, K. Renin Roy, G. S. Aravind, S. Dija & Krithi Manohar. (2023). Digital Forensics Analysis of a Vehicle Tracking System. SN Computer Science. Springer.

28. Shenqing Wang, Jiang Wang, Chunhua Su & Xinshu Ma. (2020). Intelligent Detection Algorithm Against UAVs' GPS Spoofing Attack. 2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS). IEEE.

29. Shenzheng Zuo, Yinan Liu, Dongmei Zhang, Pengpeng Xin & Tianxin Liu. (2021). Detection of GPS Spoofing Attacks Based on Isolation Forest. 2021 IEEE 9th International Conference on Information, Communication and Networks (ICICN). IEEE.

30. Ibraheem I. K. & Hadi S. W. (2018, May). Design and implementation of a low-cost secure vehicle tracking system. 2018 IEEE *International Conference on Engineering Technology and their Applications (IICETA).* (pp. 146-150). IEEE.

31. Gupta, Shreya & Ginni Arora. (2019). Use of homomorphic encryption with GPS in location privacy. 2019 *4th International Conference on Information Systems and Computer Networks (ISCON)*. IEEE.

32. Daven Darmawan Sendjaya, Fathiya Amani Shabira, Maritza Humaira, Muhammad Raihan Elfazri & Muhammad Ogin Hasanuddin. (2023). Development of an ESP32-Based Tracker with XTEA-Encrypted Coordinates. 2023 International Conference on Electrical Engineering and Informatics (ICEEI). IEEE.

33. Ashish Nanda, Priyadarsi Nanda, Xiangjian He, Aruna Jamdagni & Deepak Puthal. (2020). A hybrid encryption technique for Secure-GLOR: The adaptive secure routing protocol for dynamic wireless mesh networks. Future Generation Computer Systems. Elsevier.

34. Christian Vitale, Nikos Piperigkos, Christos Laoudias, Georgios Ellinas, Jordi Casademont, Josep Escrig, Andreas Kloukiniotis, Aris S. Lalos, Konstantinos Moustakas, Rodrigo Diaz Rodriguez, Daniel Baños, Gemma Roqueta Crusats, Petros Kapsalas, Klaus-Peter Hofmann & Pouria Sayyad Khodashenas. (2021). CARAMEL: results on a secure architecture for connected and autonomous vehicles detecting GPS spoofing attacks. EURASIP Journal on Wireless Communications and Networking. Springer.

35. Xiaodong Zheng, Qi Yuan, Bo Wang & Lei Zhang. (2022). A Homomorphic Encryption Based Location Privacy Preservation Scheme for Crowdsensing Tasks Allocation. Wireless Personal Communications. Springer.

36. Dang, T. N., & Vo, H. M. (2019, February). Advanced AES algorithm using dynamic key in the internet of things system. *2019 IEEE 4th international conference on computer and communication systems (ICCCS)* (pp. 682-686). IEEE.

37. Feng, C., Yu, K., Aloqaily, M., Alazab, M., Lv, Z., & Mumtaz, S. (2020). Attribute-based encryption with parallel outsourced decryption for edge intelligent IoV. *Transactions on Vehicular Technology*. IEEE.

38. Yan Cui, Siqi Li, Yue Wang & Bolin Gao. (2020). The Data Protection of Intelligent Connected Vehicles Cloud Control Framework Using Fully Homomorphic Encryption.2020 4th CAA International Conference on Vehicular Control and Intelligence (CVCI). IEEE.

39. Wanli Xue, Chengwen Luo, Yiran Shen, Rajib Rana, Guohao Lan, Sanjay Jha, Aruna Seneviratne & Wen Hu. (2020). Towards a Compressive-Sensing-Based Lightweight Encryption Scheme for the Internet of Things. IEEE Transactions on Mobile Computing. IEEE.

40. Jiawei Zhang, Teng Li, Mohammad S. Obaidat, Chi Lin & Jianfeng Ma. (2021). Enabling Efficient Data Sharing With Auditable User Revocation for IoV Systems. IEEE Systems Journal. IEEE.

41. Hassan Karim & Danda B. Rawat. (2021). TollsOnly Please—Homomorphic Encryption for Toll Transponder Privacy in Internet of Vehicles. IEEE Internet of Things Journal. IEEE.

42. Baee, M. A. R., Simpson, L., Boyen, X., Foo, E., & Pieprzyk, J. (2022). ALI: Anonymous lightweight inter-vehicle broadcast authentication with encryption. *Transactions on Dependable and Secure Computing*. IEEE.

43. Zhuangjun Ma, Shuaiyu Zhou & Bohua Yu. (2023). Applied Research on Attribute-Based Encryption Scheme with Two-level Encryption. 2023 IEEE 3rd International Conference on Data Science and Computer Application (ICDSCA). IEEE.

44. Qi Mu, Hongliang Wang, Shengcai Lu, Yu Fang, Zhangzhao He & Wei Liu.(2023). Implementation of FPGA Cipher Card Supporting SR-IOV. 2023 International Conference on Mobile Internet, Cloud Computing and Information Security (MICCIS). IEEE.

45. Zhuoqun Xia, Lingxuan Zeng, Ke Gu, Chao Su, Hangyu Hu & Kejun Long. (2023). Secure and Lightweight Vehicular Privacy Preservation Scheme Under Fog Computing-Based IoVs. IEEE Transactions on Intelligent Vehicles. IEEE.

46. Yuhong Li, Ruoyu Chen & Rahim Rahmani. (2023). Secure Data Sharing in Internet of Vehicles Based on Blockchain and Attribute-Based Encryption. 2023 IEEE International Conference on Smart Internet of Things (SmartIoT). IEEE.

47. Wei Tong & Huan Xie. (2023). Vehicle Driving Position Data Encryption Storage Method Based on Internet of Vehicles. 2023 IEEE International Conference on Sensors, Electronics and Computer Engineering (ICSECE). IEEE.

48. Manjari Singh Rathore, M. Poongodi, Praneet Saurabh, Umesh Kumar Lilhore, Sami Bourouis, Wajdi Alhakami, Jude Osamor & Mounir Hamdi. (2022). A novel trust-based security and privacy model for Internet of Vehicles using encryption and steganography. Computers and Electrical Engineering. Elsevier.

49. Pengshou xie, Haoxuan Yang, Tao Feng & Yan Yan. (2022). Implementing efficient attribute encryption in IoV under cloud environments. Computer Networks. Elsevier.

50. Xiantong Huang, Lang Li, Hong Zhang, Jinling Yang & Juanli Kuang. (2024). IoVCipher: A low-latency lightweight block cipher for internet of vehicles. Ad Hoc Networks. Elsevier.

51. Rashad Elhabob, Mazin Taha, Hu Xiong, Muhammad Khurram Khan, Saru Kumari & Pradeep Chaudhary. (2024). Pairing-free certificateless public key encryption with equality test for Internet of Vehicles. Computers and Electrical Engineering. Elsevier.

52. Yun Wu, Liangshun Wu & Hengjin Cai. (2023). Cloud-edge data encryption in the internet of vehicles using Zeckendorf representation. Journal of Cloud Computing. Springer.

53. Ling Xing, Yuanhao Huang, Jianping Gao, Xiaofan Jia, Honghai Wu & Huahong Ma . (2023). Location Entropy-Based Privacy Protection Algorithm for Social Internet of Vehicles. Wireless Personal Communications. Springer.

54. Yashar Salami, Vahid Khajehvand & Esmaeil Zeinali. (2024). A new secure offloading approach for internet of vehicles in fog-cloud federation. Scientific Reports. Springer.

55. Milan Milenkovic. (2020). Internet of Things: Concepts and System Design. *Computer Science*. Springer.

56. Rolando Herrero. (2023). Practical Internet of Things Networking: Understanding IoT Layered Architecture. *Springer*.

57. Vishnu Kumar, Adnan Ali, Akula Zaheer Sha & Siddem Rajesh. (2024). IoT based Intelligent Systems for Vehicle. 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT). IEEE.

58. Jinliang Wang, Jingfei Wang, Zhengtang Zhu, Jin Qin, Wang Yuan, Hao Zhang, Youpeng Fan, Chaonan Liu, Wendong Niu & Sai Li. (2021). Research on Construction of the Smart Internet of Vehicles. 2021 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS). IEEE.

59. Shiho Kim & Rakesh Shrestha. (2020). Automotive Cyber Security: Introduction, Challenges, and Standardization. Springer.

60. Abubakar Saad, Penghan Yan & Robson E. (2023). MDP-based connectivity and availability models for Internet of Vehicles. Internet of Things. Elsevier.

61. Navin Kumar, Sandeep Kumar Sood & Munish Saini, (2023). Internet of Vehicles (IoV) based Framework for Vehicle Degradation using Multidimensional Dynamic Time Warping (MDTW). Expert Systems with Applications, Elsevier.

62. Navin Kumar, Sandeep Kumar Sood & Munish Saini. (2024). Internet of Vehicles (IoV) Based Framework for electricity Demand Forecasting in V2G. Energy. Elsevier.

63. Liu Y., Pan L. & Chen S. (2023). A hierarchical blockchain-enabled security-threat assessment architecture for IoV. Digital Communications and Networks. Elsevier.

64. Arooj A., Farooq M. S., Umer T., Rasool G. & Wang B. (2020). Cyber physical and social networks in IoV (CPSN-IoV): A multimodal architecture in edge-based networks for optimal route selection using 5G technologies. IEEE Access, 8, 33609-33630. IEEE.

65. Ang L. M., Seng K. P., Ijemaru G. K. & Zungeru A. M. (2018). Deployment of IoV for smart cities: Applications, architecture, and challenges. IEEE access, 7, 6473-6492. IEEE.

66. Azzahar D.M.M., Darus M., Elias S.J., Jasmis J., Zakaria M.Z. & Dawam S.R.M. (2020). A Review: Standard Requirements for Internet of Vehicles (IoV) Safety Applications. 2020 5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE). IEEE.

67. Min Wang & Sinan Wang. (2021).Communication Technology and Application in Internet of Vehicles. IEEE. 2021 IEEE 4th International Conference on Information Systems and Computer Aided Education (ICISCAE). IEEE.

68. Xudong Tan, Wei Cheng, Haiping Huang, Tianyi Jing & Haiyan Wang. (2023). Edge-aided searchable data sharing scheme for IoV in the 5G environment. Journal of Systems Architecture. Elsevier.

69. Hamid, U. Z. A., Zamzuri, H., & Limbu, D. K. (2019). Internet of vehicle (IoV) applications in expediting the implementation of smart highway of autonomous vehicle: A survey. Performability in Internet of Things, 137-157. Springer.

70. Priyanka Mishra & Ghanshyam Singh. (2023). Internet of Vehicles for Sustainable Smart Cities. Sustainable Smart Cities. Springer.

71. Nibedita Priyadarsini Mohapatra & Sudhir Ranjan Pattanai. (2023). Green Internet of Vehicles (GIoV): Applications, Awareness, Technologies and Challenges. 2023 IEEE 3rd International Conference on Sustainable Energy and Future Electric Transportation (SEFET).IEEE.

72. Eugen Borcoci, Ana-Maria Drăgulinescu, Frank Y. Li, Marius-Constantin Vochin & Kjetil Kjellstadli. (2021). An Overview of 5G Slicing Operational Business Models for Internet of Vehicles, Maritime IoT Applications and Connectivity Solutions. IEEE Access. IEEE.

73. Shiho Kim & Rakesh Shrestha. (2020). Automotive Cyber Security: Introduction, Challenges, and Standardization. Springer.

74. Hani AlGhanem & Sherief Abdallah. (2024). The Future of the Internet of Vehicles (IoV). Springer.

75. Kamble, S. J., & Kounte, M. R. (2023). Trends and Open Research Issues in Intelligent Internet of Vehicles. Transport and Telecommunication Journal, 24(2), 143-157. Sciendo.

76. Michael Georgiades & Marios S. Poullas. (2023). Emerging Technologies for V2X Communication and Vehicular Edge Computing in the 6G era: Challenges and Opportunities for Sustainable IoV. 2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT). IEEE.

77. Phibadeity S. Marwein & Debdatta Kandar. (2023). A Novel Load Balancing Approach in Internet of Vehicles (IoV). 2023 4th International Conference on Computing and Communication Systems (I3CS). IEEE.

78. Madhusudan Singh. (2021). Information Security of Intelligent Vehicles Communication: Overview, Perspectives, Challenges, and Possible Solutions. Springer.

79. Abhay Garg, Aditya Chauhan & Prashant Giridhar Shambharkar. (2022). Security Threats & Attacks in IoV Environment: Open Research Issues and Challenges. 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT). IEEE.

80. Taslimasa H., Dadkhah S., Neto E.C.P., Xiong P., Ray S., Ghorbani A.A. (2023). Security issues in Internet of Vehicles (IoV): A comprehensive survey. Internet of Things. Elsevier.

81. Tao Hai, Muammer Aksoy, Celestine Iwendi, Ebuka Ibeke & Senthilkumar Mohan. (2024). CIA Security for Internet of Vehicles and Blockchain-AI Integration. Journal of Grid Computing. Springer.

82. Vijayakumar Gali, Mariana Resener & Madisa V.G. Varaprasad. (2024). Advanced Technologies in Electric Vehicles: Challenges and Future Research Developments. Elsevier.

83. Hyunghoon Kim, Yeonseon Jeong, Wonsuk Choi, Doon Hoon Lee & Hyo Jin Jo. (2022). Efficient ECU Analysis Technology Through Structure-Aware CAN Fuzzing. IEEE Access. IEEE.

84. Bhupendra Teriya & Sushma Gupta. (2023). ECU Testing for Safe Power Supply in Car with Vector Tools and Hardware-in-Loop. 2023 IEEE Renewable Energy and Sustainable E-Mobility Conference (RESEM). IEEE.

85. Gupta S. K. (2020). A Textbook of Automobile Engineering. S. Chand Publishing.

86. Masaru Matsubayashi, Takuma Koyama & Masashi Tanaka. (2023). In-Vehicle Network Inspector Utilizing Diagnostic Communications and Web Scraping for Estimating ECU Functions and CAN Topology. IEEE Access. IEEE.

87. Marieta Yordanova & Aydan Haka. (2023). Comparative Evaluation of Communication Protocols in the Automotive Industry. 2023 18th Conference on Electrical Machines, Drives and Power Systems (ELMA). IEEE.

88. Akib Anwar, Anika Anwar, Lama Moukahal & Mohammad Zulkernine. (2023). Security assessment of in-vehicle communication protocols. Vehicular Communications. Elsevier.

89. Mahmood Zaigham. (2020). Connected vehicles in the internet of things: Concepts, Technologies and Frameworks for the IoV. Cham, Switzerland: Springer.

90. Yan Wang, Yufei Zhang & Xiaoyan Huang. (2023). Development and Teaching Application of an Intelligent Connected Vehicle Comprehensive Road Testing Connected Control Platform. 2023 3rd International Conference on Digital Society and Intelligent Systems (DSInS). IEEE.

91. Dong-Fan Xie, Yong-Qi Wen, Xiao-Mei Zhao, Xin-Gang Li & Zhengbing He. (2020). Cooperative driving strategies of connected vehicles for stabilizing traffic flow. Taylor & Francis.

92. Bousbaa F.Z., Kerrache C.A., Lagraa N., Hussain R., Yagoubi M.B., Tahari A.E.K. (2022). Group data communication in connected vehicles: A survey. Vehicular Communications. Elsevier.

93. Kanghua Ma, Shubing Liao & Yunyun Niu. (2024). Connected vehicles' dynamic route planning based on reinforcement learning. Future Generation Computer Systems. Elsevier.

94. Ji, B., Zhang, X., Mumtaz, S., Han, C., Li, C., Wen, H., & Wang, D. (2020). Survey on the internet of vehicles: Network architectures and applications. Communications Standards Magazine, 4(1), 34-41. IEEE.

95. Rezki Assem, Guezouli Lyamine, Benyahia Abderrezak, Seghir Zineb & Lamraoui Abdelkrim. (2023). Data Processing from VANETs to IoV: Literature Review. Springer.

96. Steven Van Uytsel & Danilo Vasconcellos Vargas. (2021). Autonomous Vehicles: Business, Technology and Law. Springer.

97. Gupta, N., Prakash, A., & Tripathi, R. (Eds.). (2021). Internet of vehicles and its applications in autonomous driving. Berlin/Heidelberg, Germany: Springer.

98. Darren Wishart, Shelly Weaver & Anna Apuli. (2023). Autonomous vehicles: What are your intentions?. Transportation Research Part F: Traffic Psychology and Behaviour. Elsevier.

99. Eva Kassens-Noor, Mark Wilson & Tan Yigitcanlar. (2021). Where Are Autonomous Vehicles Taking Us?. Journal of Urban Technology. Taylor & Francis.

100. Zhiwei Sun, Miao Lin, Wentao Chen, Bing Dai, Pengfei Ying & Qing Zhou. (2024). A case study of unavoidable accidents of autonomous vehicles. Traffic Injury Prevention. Elsevier.

101. Chade Saghir & Gary Sands. (2020). Realizing the Potential of Autonomous Vehicles. Planning Practice & Research. Taylor & Francis.

102. Jing Yang, Qinghua Ni, Guiyang Luo, Qi Cheng, Latifa Oukhellou & Shuangshuang Han. (2023). A Trustworthy Internet of Vehicles: The DAO to Safe, Secure, and Collaborative Autonomous Driving. IEEE Transactions on Intelligent Vehicles. IEEE.

103. Xinyu Zhang, Jun Li, Zhiwei Li, Huaping Liu, Mo Zhou, Li Wang, Zhenhong Zou. (2023). Multi-sensor Fusion for Autonomous Driving. Singapore: Springer.

104. George Dimitrakopoulos, Aggelos Tsakanikas & Elias Panagiotopoulos. (2021). Autonomous Vehicles: Technologies, Regulations, and Societal Impacts. Elsevier.

105. Shiho Kim & Rakesh Shrestha. (2020). Automotive Cyber Security: Introduction, Challenges, and Standardization. Springer Singapore. Springer.

106. Alfonso Martínez-Cruz, Kelsey A. Ramírez-Gutiérrez, Claudia Feregrino-Uribe & Alicia Morales-Reyes. (2021). Security on in-vehicle communication protocols: Issues, challenges, and future research directions. Computer Communications. Elsevier.

107. Haotong Cao, Sahil Garg, Georges Kaddoum, Mohammad Mehedi Hassan & Salman A. AlQahtani. (2022). Secure and intelligent slice resource allocation in vehicles-assisted cyber physical systems. Computer Communications. Elsevier.

108. Abdulrahman Abu Elkhail, Rafi Ud Daula Refat, Ricardo Habre, Azeem Hafeez, Anys Bacha & Hafiz Malik. (2021). Vehicle Security: A Survey of Security Issues and Vulnerabilities, Malware Attacks and Defenses. IEEE Access. IEEE.

109. Jun Sun, Dong Liu, Yang Liu, Chuang Li & Yumeng Ma. (2022). Research on the Characteristics and Security Risks of the Internet of Vehicles Data. 2022 7th IEEE International Conference on Data Science in Cyberspace (DSC). IEEE.

110. Jingxiu Xu, Meiyan Li, Zhonglin He & Tomley Anwlnkom. (2023). Security and privacy protection communication protocol for Internet of vehicles in smart cities. Computers and Electrical Engineering. Elsevier.

111. Aifen Sui & Gordon Muehl. (2020). Security for Autonomous Vehicle Networks. 2020 IEEE 3rd International Conference on Electronic Information and Communication Technology. IEEE.

112. Teena Kumari, Abdur Rakib, Arkady Zaslavsky, Hesamaldin Jadidbonab & Valeh Moghaddam. (2024). A Context-Aware Framework for Analysing Automotive Vehicle Security. 2024 IEEE 18th International Conference on Semantic Computing (ICSC). IEEE.

113. Joseph Migga Kizza. (2024). Guide to Computer Network security. Berlin: Springer.

114. Fargana Abdullayeva. (2023). Cyber resilience and cyber security issues of intelligent cloud computing systems. Results in Control and Optimization. Elsevier.

115. M Kokila & Srinivasa Reddy K. (2024). Authentication, access control and scalability models in Internet of Things Security–A review. Cyber Security and Applications. Elsevier.

116. Harun Ecik. (2021). Comparison of Active Vulnerability Scanning vs. Passive Vulnerability Detection. 2021 International Conference on Information Security and Cryptology (ISCTURKEY). IEEE.

117. Sihn-Hye Park, Dongyoon Kim & Seok-Won Lee. (2023). A Tool for Security Risk Assessment for APT Attacks: using Scenarios, Security Requirements, and Evidence. 2023 IEEE 31st International Requirements Engineering Conference (RE). IEEE.

118. Eric Conrad, Seth Misenar & Joshua Feldman. (2023). CISSP® Study Guide. Elsevier.

119. Ramchandra Sharad Mangrulkar , Pallavi Vijay Chavan. (2024). Blockchain Essentials: Core Concepts and Implementations. Springer.

120. Saravanan Krishnan, Valentina E. Balas & Raghvendra Kumar. (2020). Handbook of Research on Blockchain Technology. Elsevier.

121. Lamia Alashaikh. (2021). Blockchain-Based Software Systems: Taxonomy Development. 2021 IEEE International Conference on Blockchain (Blockchain). IEEE.

122. Zhong Xu &Chuanwei Zou. (2020). What can blockchain do and cannot do?. Taylor & Francis.

123. Robin Sharp.(2024). Introduction to Cybersecurity: A Multidisciplinary Challenge. Springer.

124. Aiden A. Bruen, Mario A. Forcinito & James M. McQuillan. (2021). Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century. IEEE.

125. Massimo Bertaccini. (2022). Cryptography Algorithms: A guide to algorithms in blockchain, quantum cryptography, zero-knowledge protocols, and homomorphic encryption. IEEE.

126. Dashuai Gao, Juping Wu & Lede Niu. (2021). A Method For Comprehensive Ability Assessment of Smart City Construction From The Perspective of Big Data. 2021 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS). IEEE