"The Future of Mobility: Exploring the Role of IoT in Connected Cars"

Research Project of SIME(Society for Industrial Management and engineering)
Made by- Maitreyi Pandey

What are connected cars?

Connected cars are vehicles equipped with internet access and communication technologies that enable them to interact with other vehicles, infrastructure, and devices. They offer features like real-time traffic updates, navigation, infotainment, remote diagnostics, and safety alerts. By using technologies like 5G and IoT, connected cars enhance driving experiences, improve safety, enable predictive maintenance, and support autonomous driving and smart city integration.

History of connected cars- “How did the idea arise

The history of connected cars dates back several decades, evolving with advancements in communication and automotive technologies:

1960s-1980s: Early vehicle communication systems like OnStar (1980s) offered emergency assistance and navigation.

1990s: Telematics systems, such as GPS, began integrating with vehicles for location tracking and roadside assistance.

2000s: BMW launched ConnectedDrive, blending internet services and driving aids.

2010s: Introduction of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. Tesla pioneered over-the-air software updates.

2020s: 5G technology, V2X communication, and AI-driven features propel connected cars toward autonomous driving and smart city integration.

Current Trends in Connected Cars

5G Technology: Enables faster, real-time data sharing and supports autonomous driving with improved connectivity.

V2X Communication: Enhanced Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Pedestrian (V2P) communication for safety and traffic management.

ADAS: AI-driven systems for adaptive cruise control, lane assistance, and automated parking.
Infotainment: Seamless smartphone integration and personalized in-car experiences using AI.

OTA Updates: Remote software upgrades for features and fixes.

Cybersecurity: Advanced encryption to protect against hacking.

EV Integration: Optimization of battery usage and charging navigation.

Data Monetization: Vehicle data used for insurance, predictive maintenance, and smart city applications.

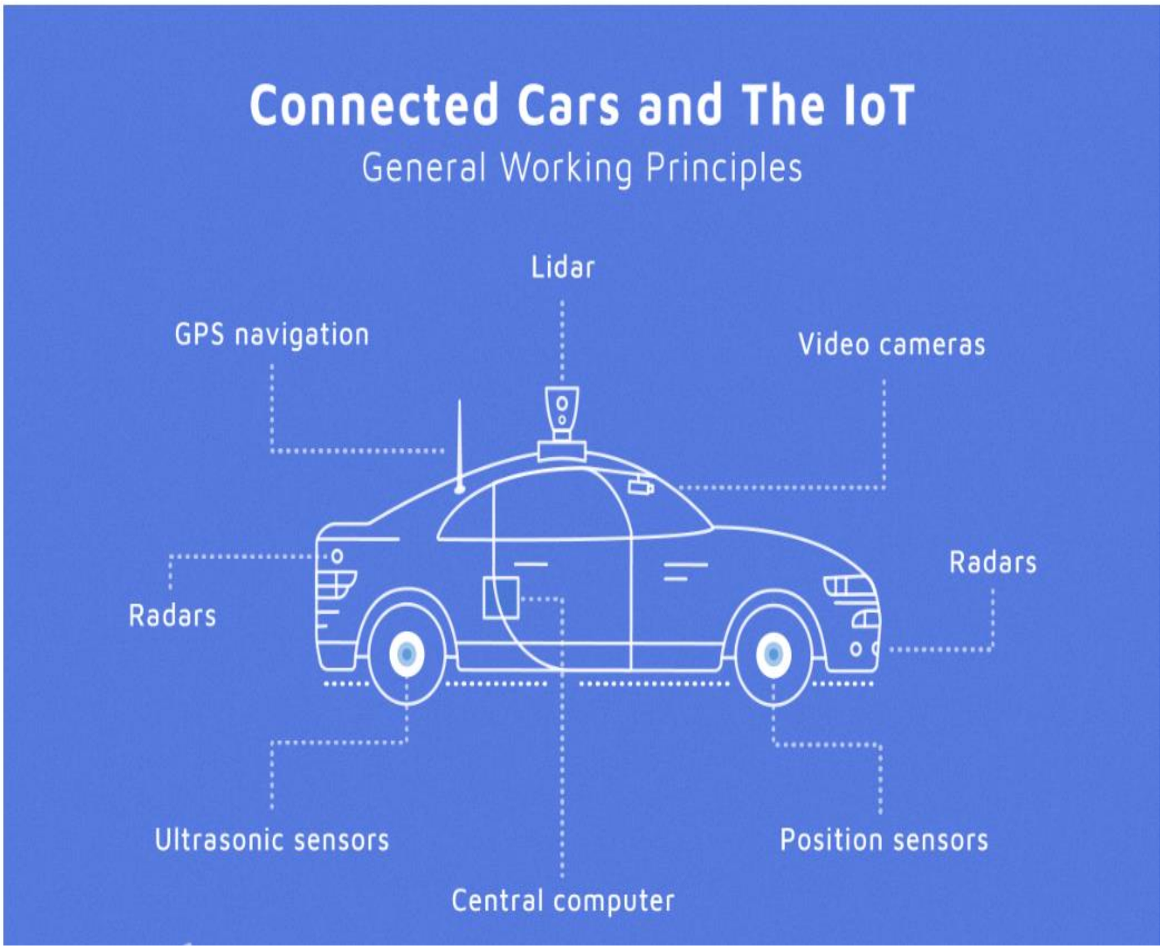
Connected cars leverage IoT, 5G, AI, and edge computing for enhanced safety, personalization, real-time data, and autonomous driving capabilities.

Why IOT in connected cars?

The Internet of Things (IoT) plays a crucial role in enabling connectivity and enhancing vehicle functionality by integrating vehicles with a network of devices, sensors, and systems. Here's how IoT achieves this:

1. Real-Time Data Collection
IoT sensors collect real-time data on vehicle performance, road conditions, and driver behavior. This data helps optimize fuel efficiency, reduce wear and tear, and improve safety.

2. Vehicle-to-Everything (V2X) Communication
IoT enables seamless communication between vehicles, infrastructure, pedestrians, and the cloud. Enhances traffic management, accident prevention, and navigation accuracy.



3. Remote Monitoring and Diagnostics
IoT systems allow remote monitoring of a vehicle's health, detecting issues before they become serious.
Predictive maintenance is enabled, reducing downtime and repair costs.

4. Smart Infotainment Systems
IoT powers personalized infotainment experiences, integrating voice assistants, streaming, and navigation.

5. Enhanced Safety Features

IoT supports Advanced Driver Assistance Systems (ADAS), offering collision warnings, lane-keeping assistance, and emergency braking.

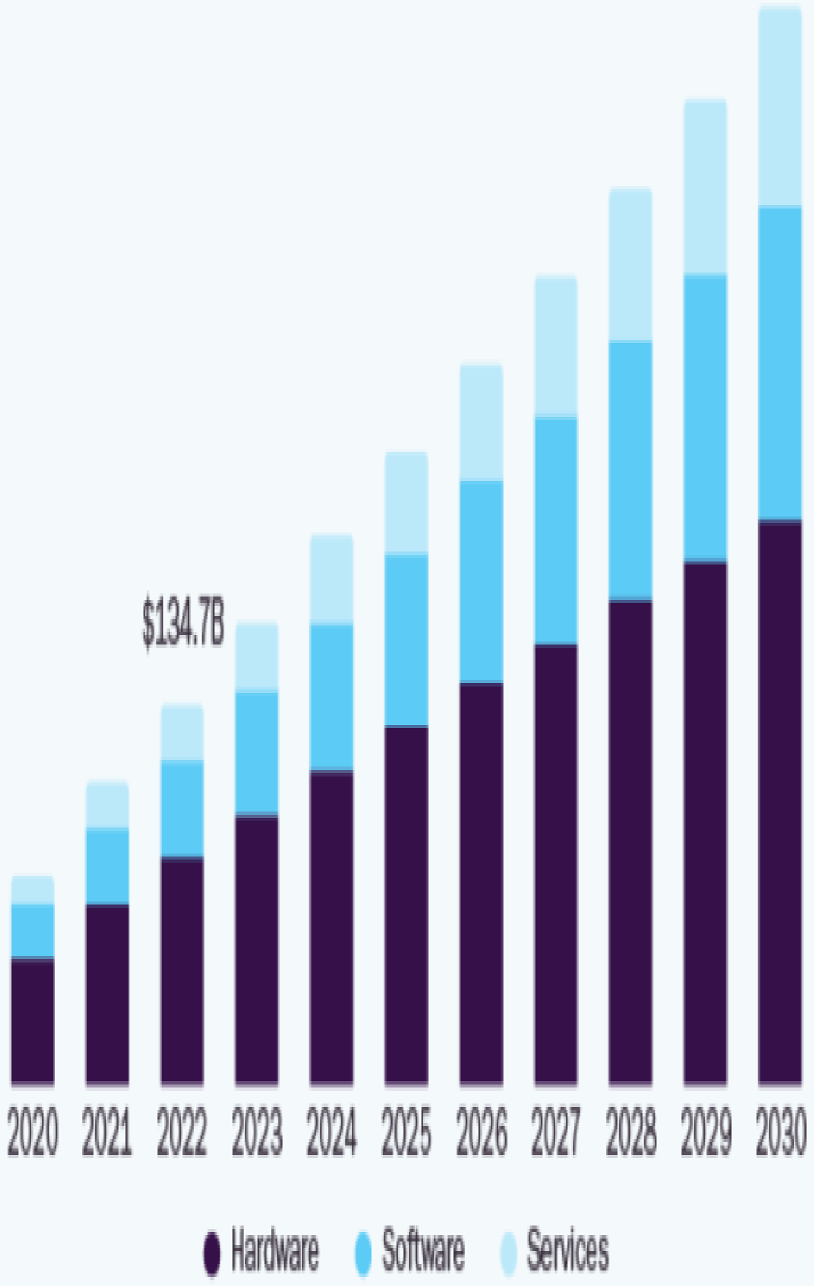
6. Over-the-Air (OTA) Updates
IoT allows vehicles to receive software updates remotely, adding features or improving performance.

7. Fleet and Resource Management
IoT enables real-time tracking, route optimization, and fuel management for fleet operators.

By connecting vehicles to a larger ecosystem, IoT significantly enhances functionality, safety, and convenience for drivers and passengers.

Automotive IoT (Internet of Things) Market Size

by Component, 2020 - 2030 (USD Billion)



GRAND VIEW RESEARCH

11.8%

Global Market CAGR, 2024 - 2030

Source:
www.grandviewresearch.com

How can connected cars can lead us to sustainable mobilty?

Improved Traffic Management: Optimizes traffic flow, reduces congestion, and prevents accidents through vehicle-infrastructure communication.

Reduced Emissions: Efficient routes and driving patterns cut fuel use and carbon emissions, supporting greener cities.

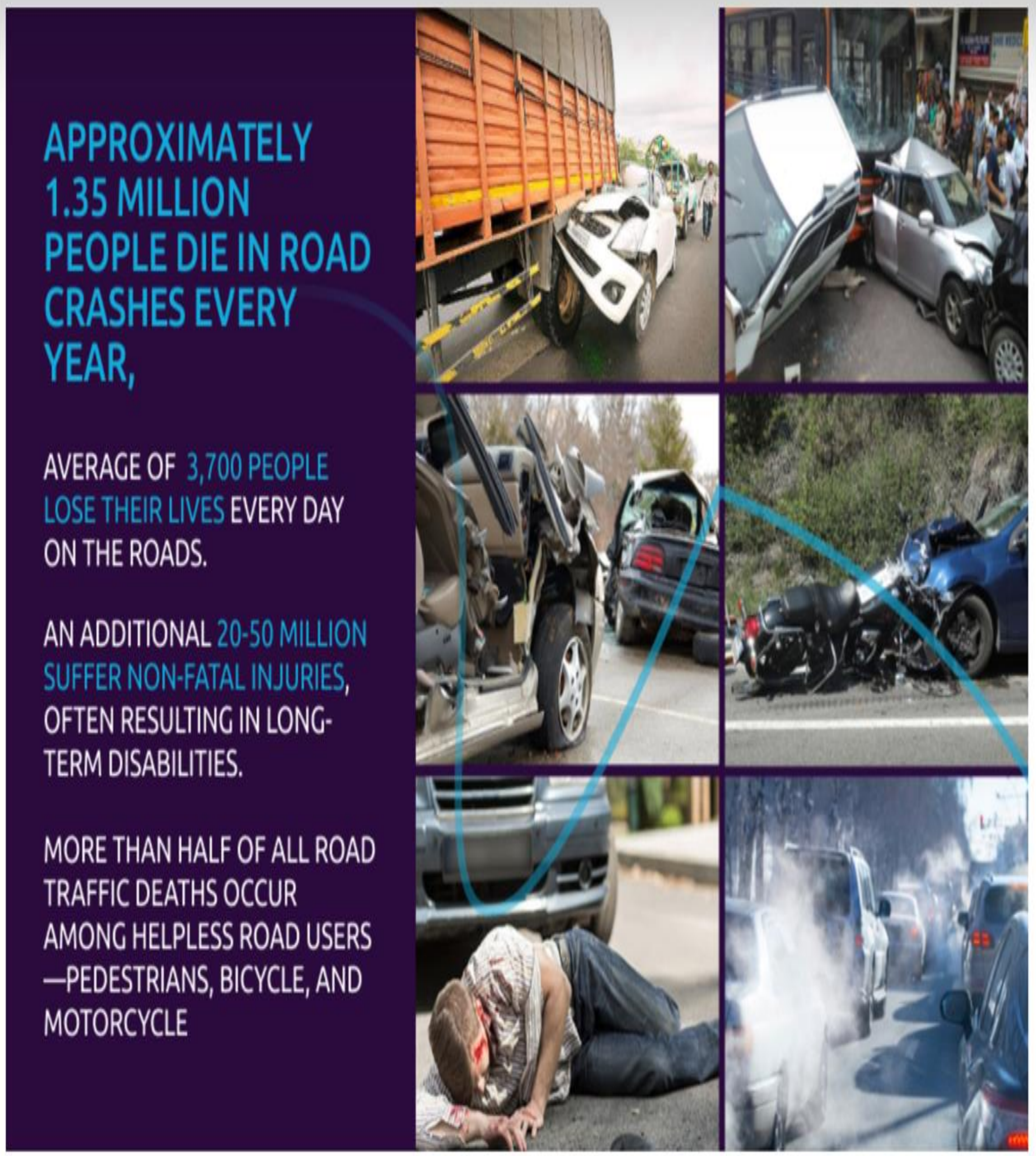
Enhanced Public Safety: Real-time data sharing alerts drivers about hazards and improves emergency response times.

Efficient Parking: Helps locate available parking spots, reducing traffic and emissions.

Integration with Autonomous Vehicles: Essential for autonomous systems, increasing safety and efficiency.

Seamless Mobility: Facilitates integration with other transport modes for smooth, multimodal transportation.
Data-Driven Planning: Provides insights for better infrastructure and sustainability planning in cities.

Connected cars contribute to safer, greener, and more efficient urban transportation systems.



APPROXIMATELY 1.35 MILLION PEOPLE DIE IN ROAD CRASHES EVERY YEAR,

AVERAGE OF 3,700 PEOPLE LOSE THEIR LIVES EVERY DAY ON THE ROADS.

AN ADDITIONAL 20-50 MILLION SUFFER NON-FATAL INJURIES, OFTEN RESULTING IN LONG-TERM DISABILITIES.

MORE THAN HALF OF ALL ROAD TRAFFIC DEATHS OCCUR AMONG HELPLESS ROAD USERS —PEDESTRIANS, BICYCLE, AND MOTORCYCLE

Core technologies and protocols that enable IoT in connected cars

1. Communication Technologies

5G: Provides high-speed, low-latency communication, essential for real-time data sharing and autonomous vehicle operation.

Wi-Fi: Used for in-car connectivity and communication with external devices or networks.

Bluetooth: Facilitates wireless connections between the vehicle and mobile devices for hands-free control and infotainment.

V2X (Vehicle-to-Everything): Enables communication between vehicles, infrastructure, pedestrians, and the cloud to improve safety and traffic flow.

2. Sensors and Actuators

GPS: Provides real-time location data for navigation and tracking.

Radar/Lidar: Used for detecting objects around the vehicle, aiding in safety features like collision avoidance.

Cameras and Ultrasound Sensors: Support features like lane-keeping assistance and parking aids.

Temperature, Pressure, and Motion Sensors: Monitor vehicle health and performance.

3. Cloud Computing and Edge Computing

Cloud: Stores and processes large amounts of data generated by connected vehicles, enabling services like remote diagnostics, software updates, and analytics.

Edge Computing: Processes data locally in the vehicle for real-time decision-making and reduced latency, crucial for safety applications.

4. Protocols

MQTT (Message Queuing Telemetry Transport): Lightweight messaging protocol used for reliable data transmission between vehicles and cloud services.

CoAP (Constrained Application Protocol): Optimized for low-power, low-bandwidth communication, commonly used in IoT devices within vehicles.

HTTP/HTTPS: Standard protocols for data exchange between connected car systems, cloud, and external services.

CAN (Controller Area Network): A robust vehicle network protocol for communication between in-vehicle systems like engine control and infotainment.

5. Security Protocols

TLS/SSL (Transport Layer Security): Ensures secure communication between vehicles and external networks, protecting data from cyber threats.

Encryption: Protects sensitive vehicle data, including location and driving behavior, from unauthorized access.

These technologies and protocols enable seamless communication, data processing, and security, making IoT in connected cars effective in enhancing safety, convenience, and efficiency.

Cybersecurity and privacy concerns associated with IoT in connected cars and challenges

The integration of IoT in connected cars brings many benefits, but it also raises significant cybersecurity and privacy concerns:

1. Unauthorized Access and Hacking
Connected cars are vulnerable to cyberattacks, where hackers can gain access to vehicle systems (e.g., braking, steering, or engine control).
Remote hacking could allow attackers to manipulate vehicle functions, putting passengers and others at risk.

2. Data Privacy Risks
Connected cars collect vast amounts of personal data (e.g., location, driving habits, and personal preferences).
If this data is not properly protected, it can be exposed to unauthorized parties, leading to privacy violations.

3. Weak Authentication and Access Control

Inadequate security measures, such as weak passwords or lack of multi-factor authentication, can make connected vehicles more susceptible to unauthorized access, especially to the onboard systems and networks.

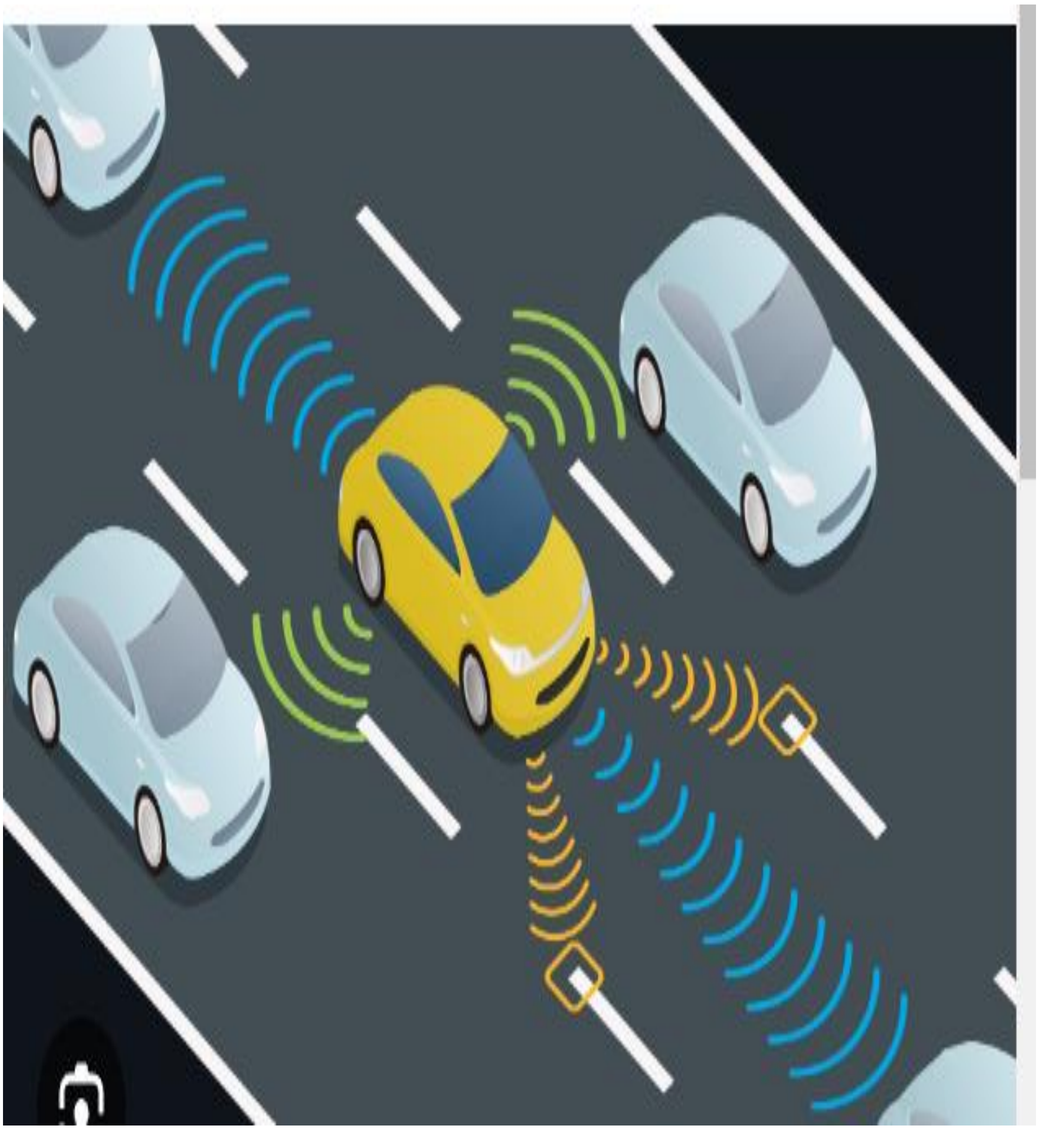
4. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Communication Risks

V2V and V2I communications can be intercepted, manipulated, or spoofed by malicious actors, leading to false traffic or safety information being shared between vehicles and infrastructure.
This can cause accidents or disruptions in traffic management.

5. Insecure Over-the-Air (OTA) Updates

OTA updates are vulnerable to tampering or interception if not properly secured.

If an attacker manages to inject malicious code into an OTA update, it could compromise vehicle systems and introduce vulnerabilities.



6. Insufficient Encryption and Data Protection
Data transmitted between the vehicle and cloud services, mobile apps, or other connected devices

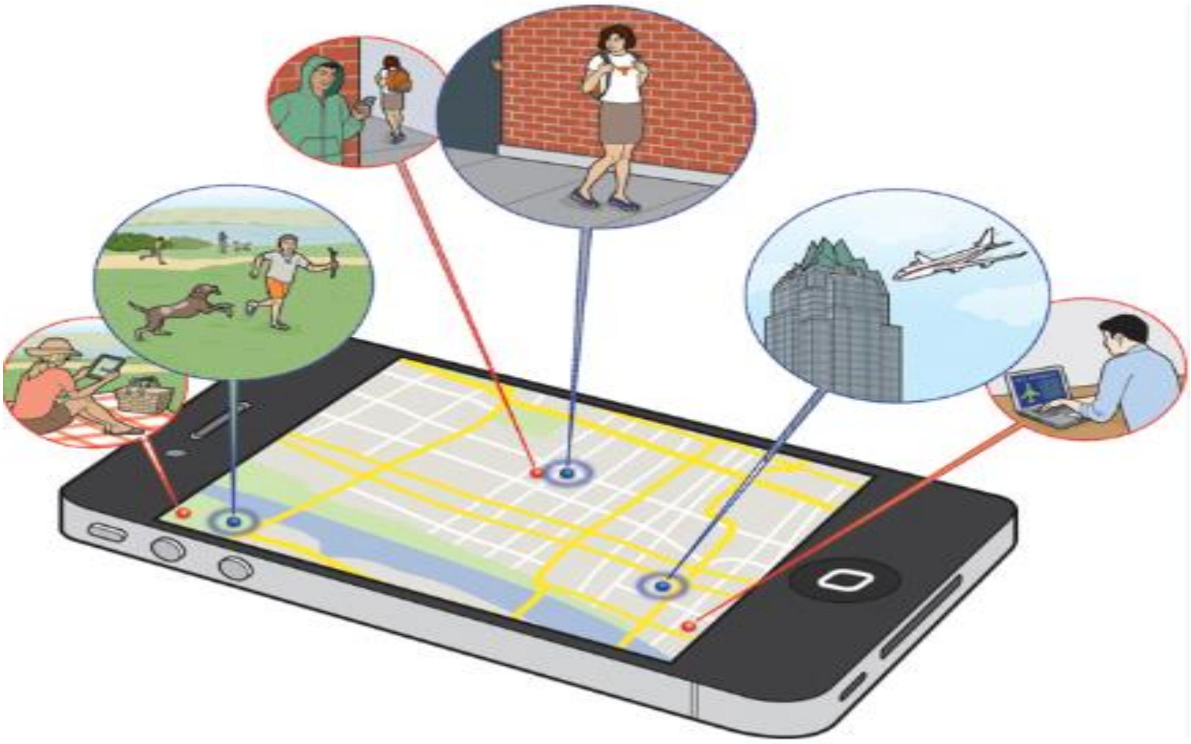
may not always be encrypted, leaving it open to interception and misuse.

7. Third-Party Services and Apps

Connected cars often rely on third-party applications and services for infotainment, navigation, or other features. These apps might not always follow stringent security protocols, potentially exposing vehicle systems to attacks.

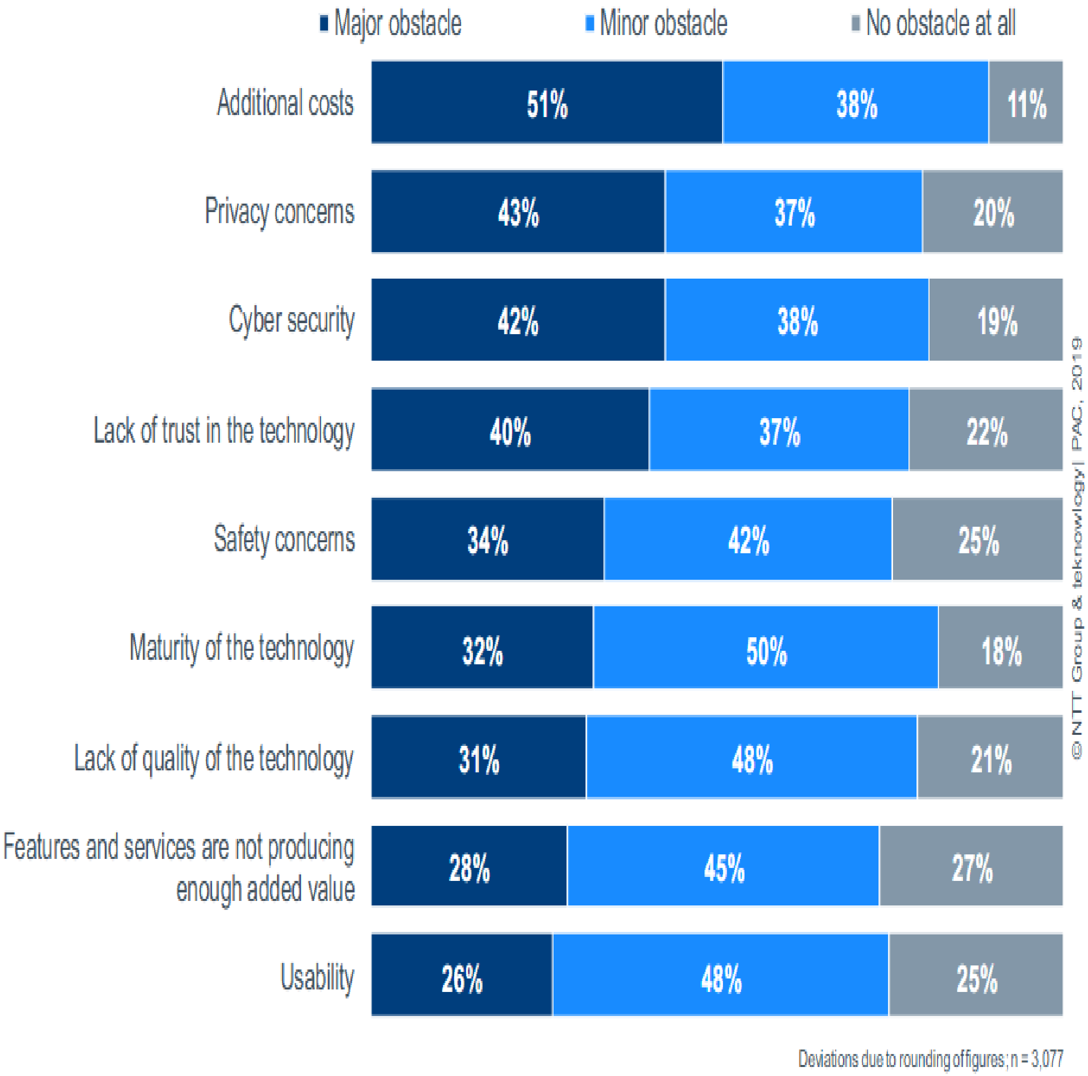
8. Location Tracking and Stalking

Constant location tracking in connected cars makes it possible for third parties to track the vehicle's movements, leading to potential stalking or unwanted surveillance.



9. Vehicle Theft and Data Breaches

If a hacker compromises a vehicle’s security system, they can steal the vehicle or access sensitive data stored in the car, like payment information or personal contacts.



Deviations due to rounding of figures; n = 3,077

© NTT Group & teknowlogy| PAC, 2019

10)High costs of implementation: Implementing IoT in connected cars incurs high costs due to advanced hardware, software integration, infrastructure development, cybersecurity measures, and continuous updates, making affordability a challenge for manufacturers and consumers.

11)Standardization and interoperability issues: Lack of standard protocols hinders seamless integration between IoT devices, creating interoperability challenges across platforms, manufacturers, and connected car ecosystems.

IoT in connected cars faces cybersecurity risks like hacking, data breaches, and unauthorized access, alongside privacy concerns regarding user data misuse. Challenges include securing networks, ensuring compliance, and maintaining user trust.

Mitigation

To overcome cybersecurity and privacy challenges in connected cars, several advancements are needed:

1)Enhanced Encryption and Secure Communication:
Adopt stronger encryption methods and secure communication standards (e.g., V2X).
Standardize secure OTA update systems and implement automated verification.

2)Improved Authentication and Access Control:
Introduce multi-factor and biometric authentication for vehicle systems.
Enhance access control measures to prevent unauthorized access.

3)Robust Intrusion Detection Systems (IDS):
Use AI and machine learning for real-time threat detection.
Monitor vehicle behavior continuously to detect anomalies.

4)Data Privacy and Management:

Implement data minimization policies and clear user consent processes.
Develop industry-wide standards for data collection and sharing.

5)Third-Party App Security:
Conduct third-party app audits and enforce security standards.
Use app sandboxing to isolate third-party apps from core systems.

6)Enhanced V2X Security:

Employ strong cryptographic protection and authentication.

Explore decentralized communication to reduce attack targets.

7)Industry Collaboration:

Develop consistent industry standards and share knowledge.
Collaborate between automakers, cybersecurity experts, and regulators.

8)Incident Response and Recovery:
Automate breach detection and response.
Create recovery plans for vehicle data and functions.

Mitigating challenges in connected cars requires enhanced encryption, regular updates, standardized protocols, cross-industry collaboration, and robust cybersecurity frameworks.

Case Study:
Pioneering Motorsport Telemetry

Discover how Control, a leader in cellular telemetry for motorsport, joined forces with Telenor IoT to redefine connectivity in endurance racing. Theirground breaking partnership ensures reliable, global telemetry coverage forelite racing teams and vehicle manufacturers.

Introduction

In the high-octane world of motorsport, precision and performance are paramount. Control, a pioneer in cellular telemetry systems for endurance racing, recognized the need for an ultra-reliable connectivity partner to take their game-changing solutions to the next level. This led to aground breaking partnership with Telenor IoT, setting new standards inthe world of motorsport telemetry.

Endurance racing demands exceptional performance, and Control’s race winning telemetry has become a game-changer Their mission to deliver precise, real-time data in the most challenging racing conditions sparked a journey that led to the creation of theTLM-P1 Evo, a groundbreaking multi-modem telemetry device. in the industry.

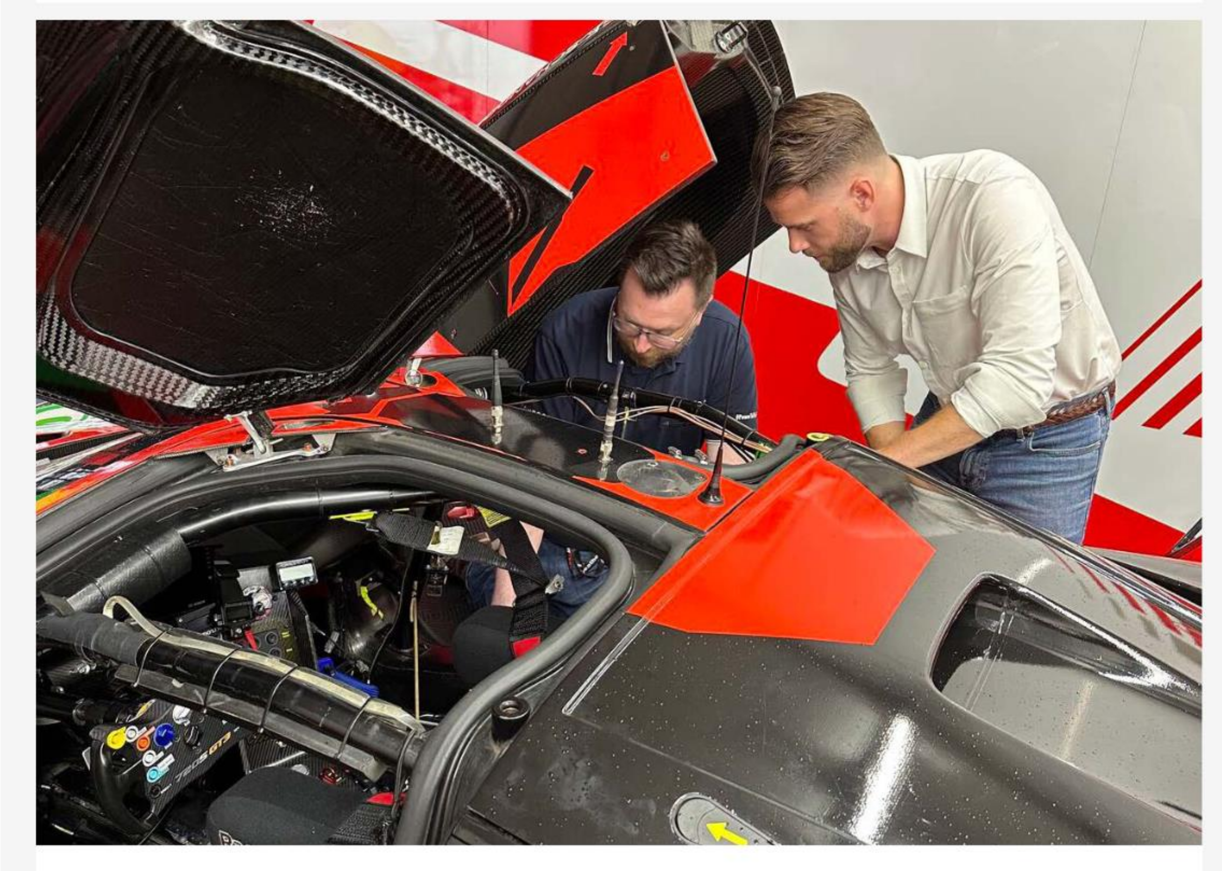
Technologically,these devices harness the power of notone but three 5G/LTE modems, each equipped with a Telenor Autograde SIM ensuring seamless connectivity to multiple cell towers and networks around the track. This innovation, backed by Telenor IoT’s managed connectivity, has been trailblazing for racing teams globally.

Background

Control’s journey has taken them to some of the world’s most renowned racetracks, in race series from FIA WEC to IMSA, providing telemetry solutions that enable elite racing teams and vehicle manufacturers to track the performance, reliability, and safety of their vehicles. At the core of Control's solution is Telenor IoT's roaming SIM, offering global telemetry coverage and the ability to race confidently in multiple countries with a single system, ensuring resilience and superior coverage.

Challenges

The world of endurance racing is unforgiving, with connectivity challenges that demand cutting-edge solutions. Racing teams require ultra-reliable connectivity and a wide selection of roaming networks. Control's vision was to provide unwavering support to their customers, offering unrivaled global telemetry coverage, but achieving this in the demanding motorsport environment was no small feat.



The partnership with Telenor IoT was ground-breaking for Control. Telenor IoT's managed connectivity provided the essential reliability, seamless roaming and connectivity to multiple networks along with API access for automation and carrier level tools for problem solving enabling Control to offer a unified product that works seamlessly worldwide. This partnership redefined what is possible in motorsport connectivity, and the results have been nothing but exceptional.

Benefits

The collaboration between Control and Telenor IoT has significant benefits:

Ultra-Reliable Connectivity: Telenor IoT's connectivity has empowered Control to provide precise, real-time data, even in the most demanding racing conditions. This ultra-reliable connection ensures that racing teams have access to critical information when it matters most.

Global Telemetry Coverage: With Telenor IoT's managed connectivity, Control's customers can confidently aim for the podium, regardless of their racing location.

Resilience & Coverage: Telenor IoT's roaming SIM ensures reliable connectivity, critical for elite racing teams.

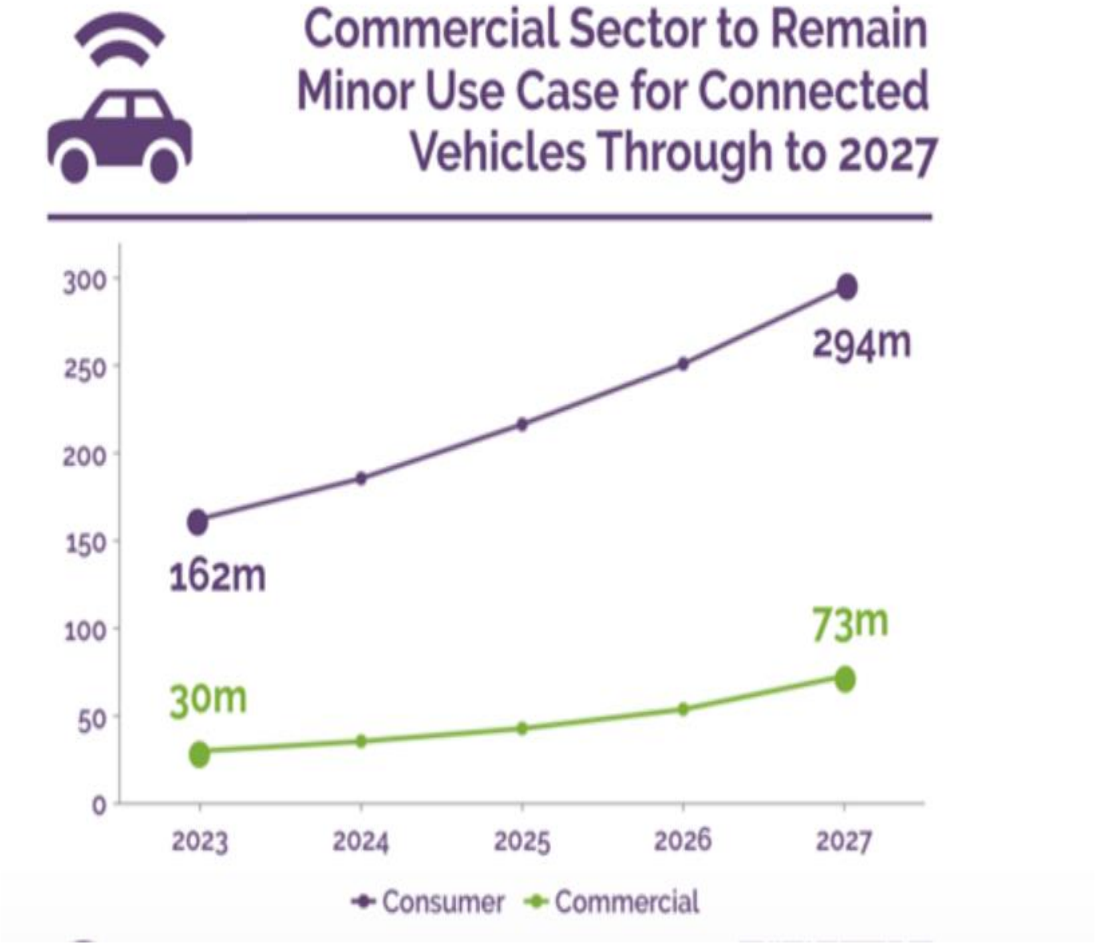
Motorsport Connectivity: The partnership with Control sets new standards for precision, reliability, and global coverage.

Leading-Edge Solutions: TLM-P1 Evo with Autograde SIMs offers uninterrupted data flow, switching networks up to 15 times per second.

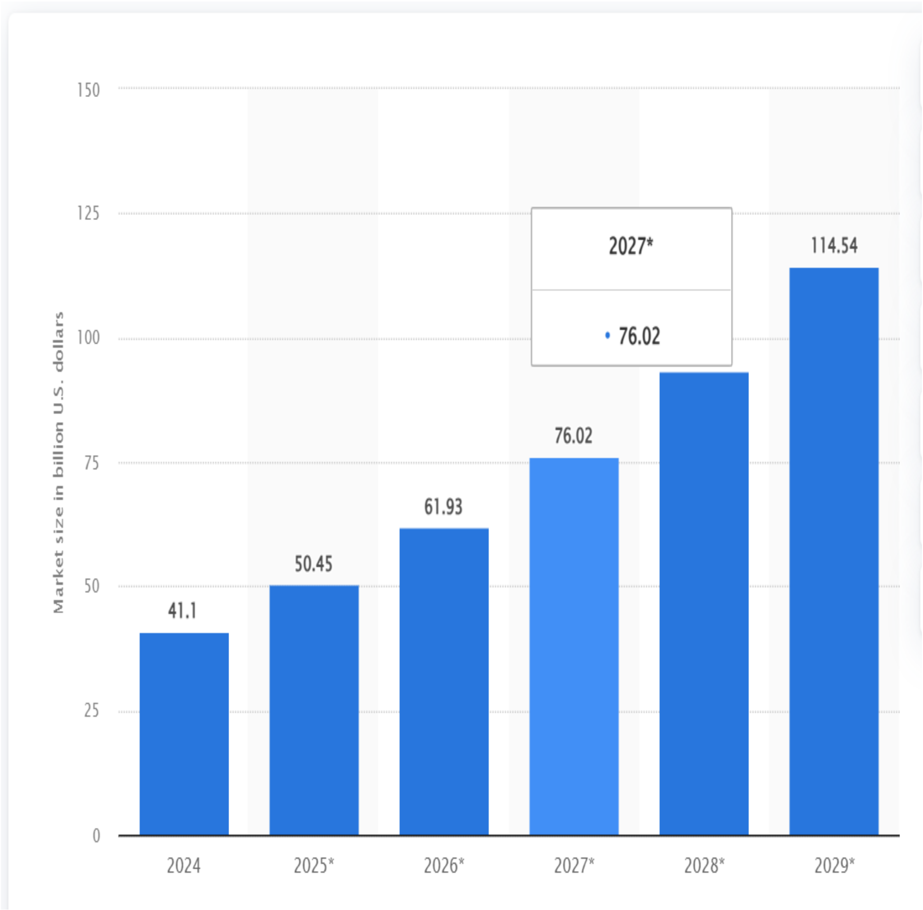
Enhanced Performance: Enables real-time decision-making for racing teams, improving track performance.

Enduring Connectivity: Telenor’s connectivity is reliable, with potential applications in various industries worldwide.

Some Statistical Data



Adoption rates of connected cars



Efficiency metrics of connected cars and iot by 2029

User experience and preferences in connected cars and iot

Personalization: Users prefer vehicles that adapt to their preferences, such as seat adjustments, climate control, and infotainment settings. IoT enables personalized profiles synced across devices.

Seamless Connectivity: Drivers value uninterrupted internet access, smartphone integration (e.g., Apple CarPlay, Android Auto), and cloud-synced navigation systems for a cohesive digital experience.

Enhanced Safety Features: Demand for IoT-powered safety features like advanced driver-assistance systems (ADAS), collision alerts, and real-time road hazard warnings is high.

Convenience and Automation: Consumers prefer automated features such as predictive maintenance alerts, remote start, and keyless entry. Voice assistants further enhance ease of use.

Real-Time Information: Users seek real-time updates on traffic, weather, and parking availability for efficient journey planning.

Sustainability: Eco-conscious drivers value IoT features that monitor fuel efficiency, suggest eco-friendly routes, and enhance electric vehicle management.

Data Privacy and Security: Increasingly, users demand robust data protection and transparency about how their personal information is used in connected systems.

Entertainment: High-quality streaming, interactive displays, and immersive audio systems are preferred for enhancing in-car entertainment.

The focus remains on creating seamless, safe, and enjoyable experiences tailored to individual preferences while addressing privacy concerns.

Future trends in IoT-enabled vehicles.

5G-Powered Connectivity: Faster and more reliable V2X (vehicle-to-everything) communication for real-time data sharing, critical for autonomous driving and smart city integration.

Edge Computing: Reduced latency with on-vehicle processing for quick decision-making in critical scenarios like collision avoidance.

Autonomous Vehicles: IoT will further enable fully self-driving cars through advanced sensor integration, AI-powered systems, and enhanced connectivity.

AI and Predictive Analytics: Enhanced user experiences with AI-driven predictive maintenance, real-time performance optimization, and personalized services.

Smart Traffic Management: IoT-enabled vehicles will integrate with smart city infrastructure to optimize traffic flow, reduce congestion, and improve urban mobility.

Over-the-Air (OTA) Updates: More frequent and secure OTA updates for software enhancements, feature upgrades, and cybersecurity patches.

Energy Efficiency and EV Integration: IoT will enhance electric vehicle (EV) management, optimize battery performance, and enable intelligent charging networks.

Enhanced In-Car Experience: AR-based navigation, immersive infotainment systems, and personalized settings powered by IoT.

Focus on Sustainability: Integration of green IoT practices to reduce emissions and align with global sustainability goals.

Cybersecurity: Advanced encryption protocols and secure frameworks to address growing concerns about data privacy and hacking risks.

These trends will drive innovation and reshape the automotive landscape toward smarter, safer, and more sustainable mobility.

Recommendations for addressing cybersecurity and standardization challenges.

1)Recommendations for Addressing Cybersecurity Challenges

Enhanced Encryption: Implement robust end-to-end encryption for data transmission between IoT devices and cloud systems.
Regular Updates: Ensure timely over-the-air (OTA) updates to address vulnerabilities and enhance security protocols.

Authentication Mechanisms: Use multi-factor authentication (MFA) and digital certificates to verify devices and users.

Secure Firmware: Adopt secure coding practices and conduct regular security audits of firmware and software.

Anomaly Detection: Deploy AI-based systems to monitor and detect unusual activities in real-time.

Collaboration: Establish partnerships between automotive, tech companies, and governments to create unified security frameworks.

2)Recommendations for Addressing Standardization Challenges

Global Standards: Develop universal IoT protocols through organizations like ISO or IEEE for seamless interoperability.

Open Ecosystems: Promote open-source platforms to encourage innovation and compatibility across devices.

Cross-Industry Collaboration: Facilitate cooperation between automakers, IoT providers, and regulators for unified standards.

Compliance Mandates: Enforce regulatory compliance for IoT integration in connected cars to ensure adherence to global benchmarks.

Testing Frameworks: Establish standardized testing and certification processes for IoT devices to ensure interoperability.

Addressing these challenges requires a balanced approach combining technology, collaboration, and regulatory measures.

Summary

IoT in connected cars is transforming mobility by enabling real-time data exchange, enhanced safety, personalized user experiences, and efficient traffic management. It supports advancements in autonomous driving, smart city integration, and sustainable transportation. Despite its potential, challenges like cybersecurity risks, high implementation costs, and lack of standardization persist. Continued research and cross-industry collaboration among automakers, tech firms, and regulators are crucial to addressing these issues, fostering innovation, and unlocking IoT's full potential in revolutionizing modern mobility.