Connected Vehicles & Security

Dr. Rakesh Das

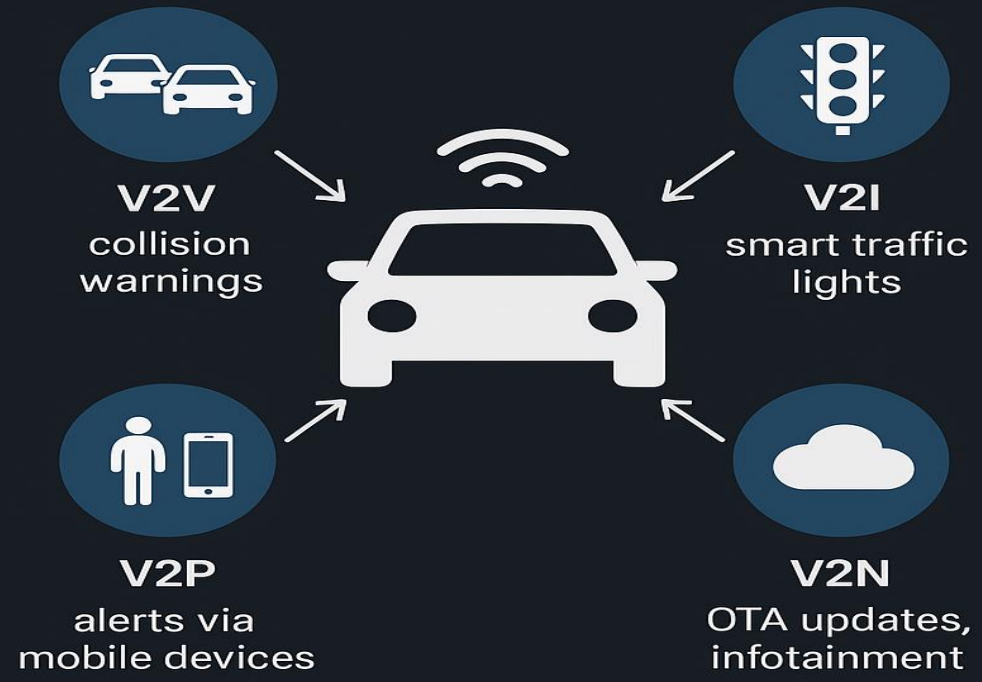
Introduction

- A **connected vehicle** is a modern automobile equipped with **embedded communication technologies and sensors** that enable it to interact with other vehicles, road infrastructure, pedestrians, networks, and cloud platforms in real time.
- It acts as part of a broader **Intelligent Transportation System (ITS)**, supporting enhanced safety, efficiency, and mobility.
- leverages **Vehicle-to-Everything (V2X)** communication to exchange safety, mobility, and **infotainment data**.
- support applications such as **collision avoidance, traffic optimization, predictive maintenance, autonomous driving, and over-the-air (OTA) updates**.

Introduction – Details

- Connected vehicles use advanced communication technologies (V2X) to exchange data with other vehicles, infrastructure, and networks. They play a critical role in intelligent transport systems and road safety.
- **Examples**
- **Tesla Model 3 / Model Y** – OTA updates, ADAS features, V2X readiness.
- **BMW Connected Drive** – real-time traffic info, remote diagnostics.
- **Toyota V2X Trials in Japan** – vehicles communicating with traffic lights for smoother flow.
- **Audi Traffic Light Information System** (U.S.) – cars “talk” to smart traffic signals in pilot cities.

CONNECTED VEHICLES



Importance of Connected Vehicles

- Enhance road safety through real-time alerts and collision avoidance.
- Improve traffic efficiency with smart routing and congestion management.
- Enable convenience via remote access, infotainment, and personalized services.
- Support sustainability by optimizing fuel use and EV integration.
- Drive innovation in autonomous driving and smart city development.

Why Security Matters

- Connected vehicles exchange vast amounts of sensitive data. Weak security can lead to hacking, data breaches, and risks to passenger safety.

🚗 **Car** – Represents connected/autonomous vehicle.

- 🔒 **Lock** – Data confidentiality & protection.
- 👤💻 **Hacker** – Cyber threats & remote attacks.
- ☁️ **Cloud** – V2X & data exchange risks.
- 🛡️ **Shield** – Cyber defense & regulations.

Connected Vehicle Ecosystem

- **Vehicles –** Smart cars with sensors and communication modules enabling V2X interactions.
- **Roadside Units (RSUs)** – Fixed infrastructure that supports V2I communication like traffic updates and hazard alerts.
- **Cloud Platforms** – Provide data storage, analytics, and OTA updates for connected mobility services.
- **Mobile Applications** – Offer user interfaces for remote control, navigation, and infotainment.
- **Government & Regulatory Frameworks** – Ensure safety, cybersecurity, and interoperability through policies and standards.

Core Technologies

- 1. Edge Computing
- 2. Digital Twin
- 3. 5G/6G
- 4. DSRC (Dedicated Short Range Communications)
- 5. Artificial Intelligence
- 6. Blockchain for security

Core Technologies

- 1. **Edge Computing:**
- “Bringing computation closer to the car for real-time decisions”
- Distributed computing paradigm.
- Data processed near the source (vehicle/roadside), not only in the cloud.
- Reduces latency, enhances reliability.

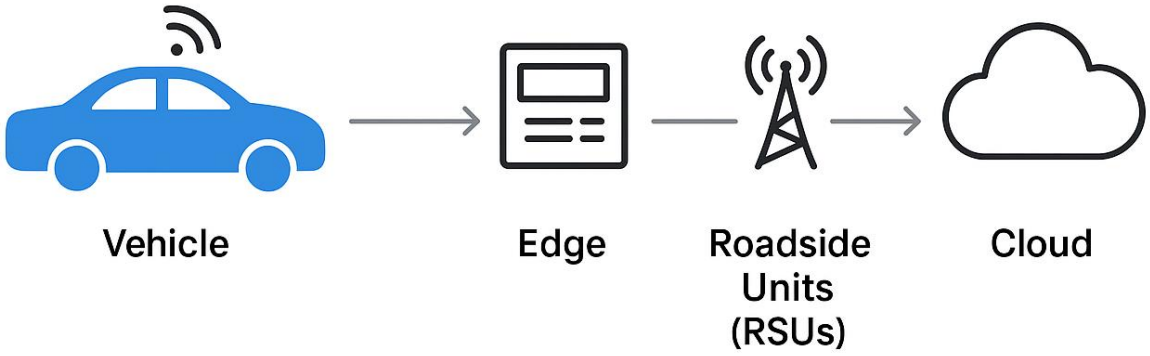
Why Edge Computing in Vehicles?

- Connected cars generate terabytes of data per day.
- Cloud-only processing → delays & bandwidth issues.
- Edge nodes (vehicles, RSUs) handle critical data locally.

Key Benefits

- Ultra-low latency (ms-level response).
- Bandwidth savings (filtering data locally).
- Increased security (local processing reduces exposure).
- Reliability (less dependent on network outages).

Edge Computing in Connected Vehicles



Core Technologies

Digital Twin:

- A new era of real-time vehicle monitoring, simulate on, and optimization.
- A Digital Twin is a virtual replica of a physical vehicle, component, or system.
- It mirrors the real-world object continuously through live data feeds.
- Used to monitor, simulate, and predict performance in connected vehicles.

How It Works

- Sensors in vehicles capture real-time data (speed, battery, engine health, tire pressure).
- Data is transmitted via 5G and Edge Computing to cloud platforms.
- A virtual twin of the vehicle is updated continuously.
- AI/ML models analyze the twin to predict failures and optimize performance.

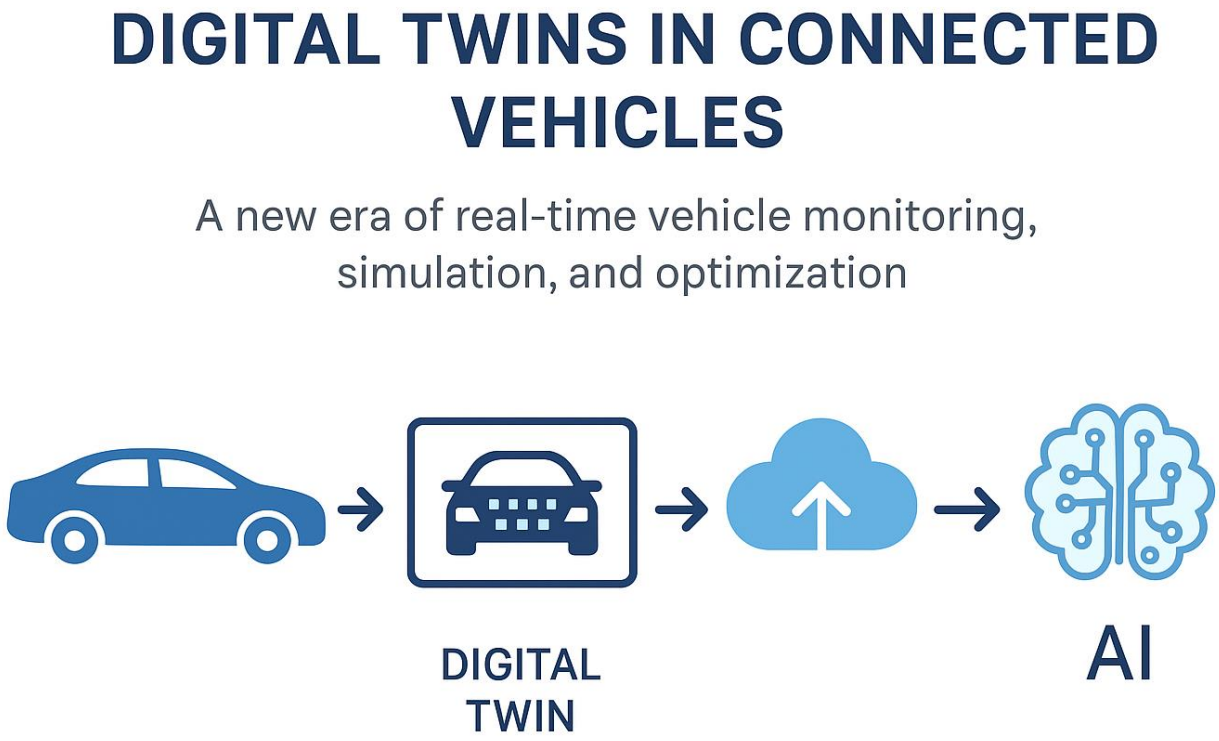
Applications

- **Predictive Maintenance** → Detect failures before they happen.
- **Crash & Safety Simulations** → Test impact scenarios digitally.
- **Performance Optimization** → Improve fuel efficiency, EV battery life.
- **ADAS Testing** → Train autonomous driving models in safe, virtual environments.
- **Fleet Management** → Monitor and optimize logistics fleets.

Benefits

- **Reduced Downtime** → Early detection prevents breakdowns.
- **Cost Savings** → Lower maintenance and repair costs.
- **Safety** → Safer testing for autonomous driving systems.
- **Continuous Improvement** → Feedback loop between physical and digital systems.
- **Data Security** → Combine with Blockchain for trusted, tamper-proof records.

Benefits


DIGITAL TWINS IN CONNECTED VEHICLES
A new era of real-time vehicle monitoring, simulation, and optimization
DIGITAL TWIN
AI

Core Technologies – Details

- **5G :**
- **Ultra-Low Latency:** Enables real-time communication between vehicles and infrastructure (<1 ms delay).
- **High Bandwidth:** Supports high data rates for HD maps, over-the-air updates, and infotainment.
- **Massive Connectivity:** Allows thousands of devices (vehicles, roadside units, sensors) to stay connected simultaneously.

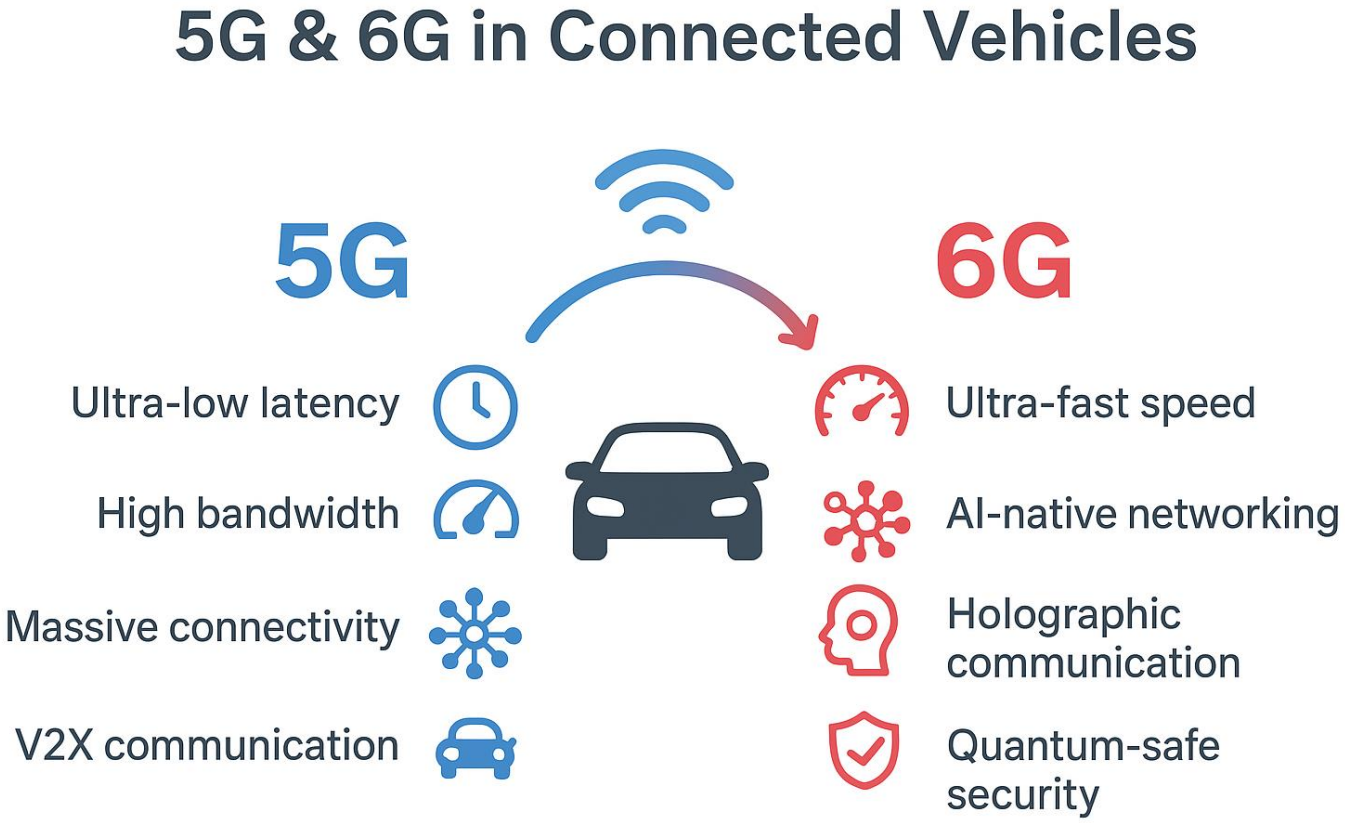
- **Applications:**
- V2X communication (vehicle-to-everything).
- Enhanced ADAS functions (collision avoidance, lane merging).
- Real-time HD video streaming for autonomous driving.

Core Technologies – Details

- **6G :**
- **Terahertz Communication:** Extremely high-frequency spectrum for ultra-fast speeds (>1 Tbps).
- **AI-Native Networking:** 6G will integrate AI at the network core for predictive, self-healing connectivity.
- **Holographic Communication:** Enables real-time holograms for remote vehicle monitoring and AR navigation.
- **Quantum-Safe Security:** Stronger cryptographic methods to secure V2X data.

- **Applications:**
- Fully autonomous mobility ecosystems.
- Smart city integration (traffic lights, drones, delivery bots).
- Seamless mixed-reality experiences inside vehicles.

Core Technologies – Details



Security Threats in Connected Vehicles

- 1. GPS Spoofing
- 2. Man-in-the-Middle Attacks
- 3. Malware & Ransomware
- 4. Denial of Service (DoS)
- 5. Sensor Spoofing

Security Threats in Connected Vehicles

GPS Spoofing

Fake GPS signals mislead vehicles

Man-in-the-Middle (MitM) Attacks

Altered data

Malware & Ransomware

Remote hijack

Denial of Service (DoS) Attacks

Network overload

Sensor Spoofing

Fake or missing objects

Security Threats in Connected Vehicles – Details

- **1. GPS Spoofing**
- Hacker secretly intercepts communication between car ↔ car or car ↔ infrastructure.
- Can alter safety-critical messages (e.g., collision alerts, traffic signals).
- Personal or vehicle data may be stolen.
- *Example:* “Green Light” signal modified to “Red Light.”

Security Threats in Connected Vehicles – Details

- **2. Man-in-the-Middle Attacks**
- Hackers broadcast fake GPS signals to mislead vehicles.
- Vehicles may follow wrong routes or misinterpret location.
- Dangerous for autonomous driving and logistics fleets.
- Example: Ships and trucks diverted by spoofed GPS signals.

Security Threats in Connected Vehicles – Details

- 3. Malware & Ransomware
- Malicious code injected via OTA update, infotainment, or USB.
- Hackers can take remote control of steering, braking, or acceleration.
- Ransomware: Driver locked out unless ransom paid.
- Example: 2015 Jeep Cherokee hack – remote hijack via entertainment system.

Security Threats in Connected Vehicles – Details

- Denial of Service (DoS)
- Flooding vehicle or RSU networks with excessive data.
- Blocks delivery of time-critical safety alerts.
- Traffic lights or emergency priority signals can be disrupted.
- Impact: Autonomous cars may stop functioning properly.

Security Threats in Connected Vehicles – Details

- 5. Sensor Spoofing
- Vehicle sensors (LiDAR, radar, cameras) tricked by false inputs.
- Creates phantom objects → unnecessary braking/lane changes.
- Can hide real objects → increases accident risks.
- Example: Fake obstacles projected on Tesla’s LiDAR.

ADAS Security Challenges

- 1. Real-time constraints
- 2. Sensor vulnerabilities
- 3. Privacy of driver data
- 4. Lack of global standards
- 5. High cost of security solutions

ADAS Security Challenges – Details

- **1. Real-time constraints**
- Vehicles need responses in milliseconds.
- Security checks must not add dangerous delays.

- **2. Sensor vulnerabilities**
- LiDAR, radar, GPS, and cameras can be spoofed.
- False signals may cause wrong driving decisions.

ADAS Security Challenges – Details

- **3. Privacy of driver data**
- Cars collect sensitive location and personal data.
- Breaches risk identity theft and data misuse.
- **4. Lack of global standards**
- Different countries use different V2X protocols.
- Lack of harmonization creates security gaps.
- **5. High cost of security solutions**
- Strong security (blockchain, IDS, secure hardware) is expensive.
- Raises vehicle cost, limiting mass adoption.

Case Study – Tesla

- Tesla uses OTA updates and AI-based monitoring. Challenges: Autopilot accidents, hacking demonstrations, regulatory concerns.
- Tesla is a pioneer in integrating **connected car technologies**.
- Known for **Over-the-Air (OTA) updates** and **AI-driven Autopilot**.
- Represents both the **potential** and **risks** of connected vehicle security.

Background

- Tesla vehicles are often described as “computers on wheels”.
- Every Tesla has a constant connection to the cloud.
- OTA updates allow Tesla to fix bugs, add features, and improve safety remotely.
- Vehicles continuously collect sensor and driving data → used for AI model training.

Technologies Used

- **1. OTA Updates**
- Allow Tesla to push new features and security patches without visiting a service center.
- Example: When hackers demonstrated remote control, Tesla patched vulnerabilities within days.
- **2. AI-Based Monitoring**
- Tesla’s Autopilot and Full Self Driving (FSD) use neural networks trained on billions of real-world miles.
- Cars use cameras + sensors for real-time decision-making.

Challenges

1. Autopilot Accidents

- Multiple cases of crashes when drivers overly relied on Autopilot.
- Raises questions about human oversight and AI limitations.

2. Hacking Demonstrations

- Researchers remotely unlocked Tesla, controlled steering/braking.
- Showed the cybersecurity risks of connected vehicles.

3. Regulatory Concerns

- Debate on whether Tesla's "Full Self Driving" name is misleading.
- Lack of global safety and legal standards for autonomous driving.

- ✔ **Strengths**
- OTA gives agility → fast response to vulnerabilities.
- AI improves continuously from massive driving data.
- ✗ **Weaknesses**
- Safety concerns due to overreliance on AI.
- Vulnerabilities open doors for hackers.
- Regulations are still catching up.
- **Key Takeaway:**
  *Tesla shows how cutting-edge tech drives innovation but also highlights why **security, ethics, and regulations** are just as important as AI and connectivity.*

Case Study – Indian Market

- Mahindra XUV700: Features like Adaptive Cruise Control & Lane Keep Assist. Challenges: Affordability & road infrastructure limitations.

Case Study – Mahindra XUV700

- Flagship SUV from Mahindra, introducing ADAS features in India.
- Represents how global ADAS technologies are adapted to Indian roads.
- Balance between innovation, affordability, and infrastructure challenges.

Background

- Launched in 2021, positioned as a tech-driven SUV.
- Among the first Indian vehicles to bring ADAS Level 2 features to the mass market.
- Competes with global automakers while addressing local road conditions and cost-sensitive buyers.

Key ADAS Features

1. Adaptive Cruise Control (ACC):

- Maintains a safe distance from the car ahead.
- Adjusts speed automatically in stop-and-go traffic.

2. Lane Keep Assist (LKA):

- Uses cameras to monitor lane markings.
- Provides steering assistance to keep the car within its lane.

3. Forward Collision Warning & Automatic Emergency Braking (AEB):

- Warns driver about potential collisions.
- Automatically applies brakes if driver does not react in time.

Challenges

Affordability

- ADAS tech increases vehicle cost, limiting adoption in price-sensitive markets.
- Buyers often prioritize mileage and affordability over advanced features.

Road Infrastructure

- Lane markings are often faded or absent in India → LKA struggles.
- Mixed traffic (bikes, autos, pedestrians) reduces ACC's effectiveness.
- Poor connectivity limits full use of connected features.

- ✔ **Strengths**
- Mahindra shows how global tech can be localized.
- Safety features like ACC and LKA are introduced at an affordable price point compared to imports.

- ✗ **Weaknesses**
- Effectiveness depends on road quality and infrastructure readiness.
- ADAS features may not perform as reliably in chaotic Indian traffic.

- 👉 **Key Takeaway:**
- The XUV700 demonstrates the potential of ADAS in emerging markets but also shows that technology must adapt to local realities like cost and infrastructure.

Security Frameworks

- 1. ISO/SAE 21434 – Road Vehicle Cybersecurity
- 2. UNECE WP.29 – International regulation
- 3. AUTOSAR Security Modules

Security Frameworks – Details

- Further elaboration on security frameworks:

- 1. ISO/SAE 21434 – Road Vehicle Cybersecurity
- 2. UNECE WP.29 – International regulation
- 3. AUTOSAR Security Modules

- Examples, diagrams, and case studies can be added here.

Cryptographic Techniques

- 1. Public Key Infrastructure (PKI)
- 2. Symmetric/Asymmetric Encryption
- 3. Blockchain for V2X authentication

Cryptographic Techniques – Details

- Further elaboration on cryptographic techniques:

- 1. Public Key Infrastructure (PKI)
- 2. Symmetric/Asymmetric Encryption
- 3. Blockchain for V2X authentication

- Examples, diagrams, and case studies can be added here.

Intrusion Detection Systems (IDS)

- Vehicle IDS monitors abnormal network traffic and anomalies. Hybrid IDS combines signature-based + behavior-based detection.

Intrusion Detection Systems (IDS) – Details

- Further elaboration on intrusion detection systems (ids):
- Vehicle IDS monitors abnormal network traffic and anomalies. Hybrid IDS combines signature-based + behavior-based detection.
- Examples, diagrams, and case studies can be added here.

Role of AI in Security

- Machine learning models detect abnormal driving or malicious data packets. AI strengthens anomaly detection and predictive security.

Role of AI in Security – Details

- Further elaboration on role of ai in security:
- Machine learning models detect abnormal driving or malicious data packets. AI strengthens anomaly detection and predictive security.
- Examples, diagrams, and case studies can be added here.

Cloud & Edge Security

- Edge computing reduces latency but poses new vulnerabilities. Cloud security ensures large-scale fleet updates and encrypted communication.

Cloud & Edge Security – Details

- Further elaboration on cloud & edge security:
- Edge computing reduces latency but poses new vulnerabilities. Cloud security ensures large-scale fleet updates and encrypted communication.
- Examples, diagrams, and case studies can be added here.

Privacy Issues

- Collection of personal driver data (location, habits). Privacy-preserving AI techniques like federated learning are being adopted.

Privacy Issues – Details

- Further elaboration on privacy issues:
- Collection of personal driver data (location, habits). Privacy-preserving AI techniques like federated learning are being adopted.
- Examples, diagrams, and case studies can be added here.

5G & Vehicle Security

- 5G enables low-latency V2X communication. Security risks: SIM cloning, network slicing attacks, rogue base stations.

5G & Vehicle Security – Details

- Further elaboration on 5g & vehicle security:

- 5G enables low-latency V2X communication. Security risks: SIM cloning, network slicing attacks, rogue base stations.

- Examples, diagrams, and case studies can be added here.

Blockchain in Connected Vehicles

- Blockchain ensures tamper-proof communication and secure identity management in V2X networks.

What is Blockchain?

- Distributed, immutable ledger.
- Records transactions in blocks linked chronologically.
- Provides tamper-proof and transparent data exchange.

Why Blockchain in Vehicles?

- V2X messages need security and authenticity.
- Prevents spoofing, fraud, and data tampering.
- Builds trust without central authority.

Applications

- **V2V Security** → Validates collision/braking alerts.
- **OTA Updates** → Prevents fake software/malware.
- **Digital Identity** → Vehicles use blockchain IDs.
- **Insurance** → Transparent accident logs.
- **Data Sharing** → Safe monetization via smart contracts.

Advantages

- Tamper-proof records.
- Decentralized & hack-resistant.
- Transparent and auditable.
- Strong authentication.

Challenges

- Scalability with millions of cars.
- Latency for real-time decisions.
- Energy use (depends on consensus).
- Integration with 5G/Edge/DSRC.
- High development cost
- Standardization issues
- Legal liability in accidents
- User trust & acceptance

Future Trends

- 1. AI-driven cybersecurity
- 2. Quantum-safe cryptography
- 3. Digital twins for vehicles
- 4. Secure Over-the-Air (OTA) updates

Conclusion

- Connected vehicles and ADAS systems will revolutionize mobility. Security is not optional but essential to ensure safety and trust.

Q&A

- Thank you! Open floor for questions.