Problems Faced on Roads & Our proposed solution

Problems Faced ⚠️

Drunk Driving

Drivers under the influence of alcohol suffer from delayed reaction times and poor judgment. Most existing systems respond only after an accident occurs, and nearby vehicles remain unaware of the risk until it is too late.

Rash / Reckless Driving

Sudden acceleration, harsh braking, and zig-zag movement significantly increase accident risk. Currently, there is no real-time mechanism to warn surrounding vehicles about such unsafe driving behaviour.

Panic-Inducing Alerts

Traditional warning methods like sirens and horns often create panic among drivers. Sudden panic braking and confusion can lead to secondary accidents and traffic disturbances.

Lack of Cooperative Vehicle Communication

Vehicles operate as isolated units without sharing safety information. The absence of a cooperative communication system prevents timely awareness and coordinated action among nearby vehicles.

💡 Our Proposed Solution

We propose **Drew's Drive -Edge AI V2X Safety node** designed to address each major road safety problem in a structured and practical manner.

Drunk Driving Detection

The system detects alcohol influence using embedded alcohol sensors and confirms unsafe behaviour through motion analysis. Once identified, the risk level is classified in real time, enabling timely intervention before an accident occurs.

Rash and Reckless Driving Monitoring

Sudden acceleration, harsh braking, and unstable vehicle movement are detected . The system continuously evaluates driving patterns and classifies the level of risk without interrupting normal driving.

Calm and Non-Panic Warning Mechanism

Instead of loud sirens or aggressive alerts, the system uses soft visual indicators and gentle audio cues. Medium risks trigger subtle click sounds, while high-risk situations activate calm voice alerts, reducing panic and secondary accidents.

Cooperative Vehicle Communication Network

Vehicles communicate using a private, vehicle-only Wi-Fi system that operates without internet access and cannot be accessed by public devices. Alerts are shared only with vehicles (V2V) within a threat radius, ensuring relevance and preventing network overload.

Authority Notification for Drunk Driving

In confirmed drunk driving cases, encrypted vehicle data and location information are securely transmitted to nearby police checkpoints, enabling timely intervention while preserving driver privacy.

This solution emphasizes **prevention without panic**, transforming independent vehicles into a cooperative safety network that enhances road safety for drivers, emergency responders, and authorities alike.

About our module:

- AES-GCM encryption is used for all vehicle-to-vehicle (V2V) communication
- Provides both confidentiality and data integrity
- Ensures alerts cannot be read or altered by unauthorized parties
- Timestamp validation ensures messages are fresh and relevant
- Replay protection prevents attackers from resending old alerts to create false warnings
- Encrypted police reporting is triggered only in confirmed drunk-driving scenarios and only within a virtual police zone, minimizing unnecessary data exposure

Security is treated as a core design requirement rather than an add-on in the Drew's Drive simulation.

Security & Encryption Keynotes

Vehicle Awareness & Threat Filtering
• Virtual GPS data simulates real road movement
• Accurate distance calculation using Haversine formula
• Directional awareness translated into simple terms (LEFT / RIGHT / FRONT / BACK)
• Threat alerts limited to operational range

Driver Risk Detection

• Alcohol sensor and MPU data are evaluated together for higher accuracy
• Short-term sensor noise is filtered using time-based stability checks
• Risk classification escalates gradually to avoid sudden or panic-inducing alerts

Key Simulation Features & Functional Highlights

The surrounding environment is emulated through virtual GPS movement, allowing the system to calculate real-world distance using the Haversine formula and determine relative direction through bearing analysis. Only vehicles within a 200-meter radius are considered, ensuring that alerts are relevant, timely, and computationally efficient. This selective processing helps maintain low latency even in dense traffic scenarios.

Once operational, the system continuously analyses alcohol sensor data combined with MPU readings to assess driver condition and vehicle stability. A ~1 second stability filter is applied to prevent false alerts caused by road vibrations or sudden steering inputs. This approach ensures that warnings are based on sustained abnormal behaviour rather than momentary noise, improving trust in the system and reducing driver distraction.

The Drew's Drive simulation demonstrates how the proposed safety module would operate in real driving environments while balancing technical reliability, security, and driver comfort. The simulation begins with a Drew's Drive splash screen, representing system startup and readiness verification. During this phase, the system performs sensor checks, initializes encryption keys, and

ensures that the display and alert mechanisms are functioning correctly before active monitoring begins.

Simulation Overview – Drew's Drive System

To ensure reliability, the system was analysed under worst-case traffic conditions to evaluate whether the ESP32 microcontroller experiences overload during operation.

In a dense traffic scenario with up to 100 vehicles within a threat radius, each vehicle transmits a compact 12-byte safety alert packet. In confirmed drunkdriving cases, an encrypted authority message of approximately 24–32 bytes is sent separately. Acknowledgement (ACK) packets of around 5 bytes are used to prevent continuous retransmission.

Even when multiple threat vehicles transmit alerts simultaneously, the ESP32 remains well within safe operating limits. The worst-case communication buffer requirement is approximately 1.1 KB, which is less than 1% of the available SRAM on the ESP32. This ensures stable memory usage without risk of overflow.

Latency analysis shows that alert transmission takes approximately 0.3 ms packet reception around 8–10 ms, and processing plus encryption roughly 5 ms. The total end-to-end response time remains within 10–20 ms, which is suitable for real-time vehicle warning systems.

The maximum estimated CPU utilization during simultaneous sensing, encryption, alert transmission, ACK handling, and dashboard indication is approximately 25–35%. Under normal driving conditions, CPU usage remains below 10%, leaving sufficient processing headroom.

Overall, the ESP32 is not overloaded under any considered scenario. The primary system limitation is wireless channel congestion due to packet

collisions in dense environments, rather than microcontroller processing capability. This confirms that the proposed system is reliable, scalable, and safe for real-world deployment.

All vehicle-to-vehicle communication is secured using AES-based symmetric encryption, ensuring that safety alerts remain confidential and cannot be interpreted or modified by unauthorized devices. Only minimal alert data, such as risk level, severity, timestamps, and temporary identifiers, is encrypted and transmitted, maintaining low latency and stable system performance.

Simulation link 🔗:Drew's Drive Simulation

Existing Technologies vs Our Proposed Technology 🔧

Existing Technologies

1. **Manual Traffic Policing**
   - Requires human intervention.
   - Not scalable or real-time.
2. **Breath Analyzers at Checkpoints**
   - Detect alcohol only after stopping vehicles.
   - Do not warn nearby traffic.
3. **Basic Vehicle Safety Features** ○ Seat belts, airbags, ABS

- Protect occupants only after impact.

4. **Traditional Emergency Sirens**
   - Audible range limited.
   - Causes panic and confusion.

🚀 Our Proposed Technology

Our system integrates embedded sensors and cooperative communication:

- MQ Alcohol Sensor – Detects alcohol presence; AI-based pattern analysis filters environmental noise and improves detection reliability over time
- Gyroscope & Accelerometer (MPU6050) – Detects rash or unstable driving; lightweight AI models analyze motion patterns to distinguish normal road disturbances from genuine risky behavior.
- ESP32 Microcontrollers – Handle sensing, preprocessing, AI inference, encryption, and vehicle-to-vehicle communication with low power consumption.
- Private Vehicle-Only Wireless Network – Enables secure, low-latency data exchange; AI-assisted traffic awareness prioritizes alerts based on risk severity and proximity.
- Distance-Based Alerts (200 m) – AI dynamically validates relevance using speed, direction, and movement context to avoid unnecessary warnings.
- Encrypted Vehicle Token – Protects driver privacy; AI-based anomaly detection flags abnormal or repeated misuse without revealing identity.

Calm Indication System

- Dashboard lights for early awareness
- Click sound for medium-risk situations

By combining sensor-based detection with lightweight AI decision support, the system improves accuracy while remaining low-cost, scalable, and practical for real-world deployment

Future Enhancement Plan

Encryption-Focused Communication

The security layer will evolve toward adaptive traffic control and intelligent filtering tightly coupled with encrypted communication. Security decisions can dynamically respond to abnormal traffic patterns, repeated authentication failures, or replay attempts without impacting normal operation. This allows suspicious nodes to be isolated early while trusted vehicles continue to exchange safety alerts seamlessly. Policy updates can be securely delivered over existing encrypted channels, avoiding manual reconfiguration. These enhancements improve resilience and stability while maintaining low latency in dense traffic environments..

Passkey-Based Key Handling

Each vehicle module is assigned a unique cryptographic passkey that establishes trust within the private vehicle network. This passkey is not transmitted during communication; instead, it is used to generate short-lived session keys for encryption and authentication. Session keys automatically expire, reducing the impact of key exposure and preventing long-term misuse.

Future improvements include lightweight dynamic key exchange and controlled passkey rotation, allowing secure key renewal as vehicles move between different traffic zones without requiring firmware changes or manual intervention.

Authentication and Replay Protection

All encrypted messages include authentication data to verify their origin and integrity. Messages that fail verification are discarded immediately. Replay attacks are prevented using timestamp validation and limited acceptance windows, ensuring that outdated alerts cannot be reused to trigger false warnings.

Encrypted acknowledgements and bounded retransmission logic prevent unnecessary wireless traffic and protect the embedded controller from overload. If any security check fails, network alerts are suppressed while local warnings continue, ensuring predictable and safe system behavior.

Privacy and Data Minimization

The system follows a data-minimization approach. No driver identity, raw sensor data, or continuous location history is transmitted. Temporary identifiers are used and periodically refreshed, reducing the possibility of long-term tracking and simplifying compliance with data-protection requirements.

Practical Industrial Deployment

For industrial use, the module will move from prototype hardware to cost-effective, automotive-suitable microcontrollers that provide improved reliability and integrated security features. These platforms support hardware-assisted encryption and secure key storage while remaining suitable for large-scale deployment and retrofitting in existing vehicles.

This transition improves long-term stability and security without significantly increasing system cost or complexity.

⭐Advantages & Benefits of the Proposed System Over ADAS

Aspect	ADAS (Advanced Driver Assistance Systems)	DREW'S DRIVE
System Focus	Works mainly on assisting a single vehicle	Works as a cooperative safety system for all nearby vehicles
Drunk Driving Detection	Indirect or limited detection based on driving behaviour	Direct detection using alcohol sensor combined with motion analysis
Rash / Reckless Driving Detection	Partial detection using lane or speed assistance	Accurate detection using gyroscope and accelerometer sensors

Vehicle-to-Vehicle Communication	Generally not supported	Actively shares warnings with nearby vehicles
Distance-Based Alerts	No proximity-based alert mechanism	Alerts activated only within a 200 m range to reduce false warnings
Alert Nature	Sudden braking or loud alerts may cause panic	Calm visual indicators, click sounds, and gentle voice alerts
Emergency Vehicle Support	No coordination with emergency vehicles	Provides early alerts to clear paths for ambulances and fire engines
Authority Notification	No integration with police or traffic authorities	Securely sends encrypted vehicle data to nearby police checkpoints
Privacy Protection	Vehicle data handled centrally by manufacturers	Uses encrypted vehicle tokens; no raw vehicle identity is broadcast
Network Dependency	Often cloud or infrastructure dependent	Operates offline using a private vehicle-only Wi-Fi network
Cost	High, limited to premium vehicles	Low-cost and suitable for wide adoption

Compatibility with Older Vehicles	Not applicable	Can be retrofitted to existing vehicles
Scalability	Limited to specific brands or ecosystems	Scalable across vehicles regardless of manufacturer
Overall Safety Impact	Improves safety of individual vehicles	Improves safety of the entire road ecosystem

---

Total Summary

This Drew's Drive introduces a **new approach to road safety**, where vehicles no longer operate independently but work together as a **cooperative safety network**.

Key highlights:

- Real-time detection of unsafe driving.
- Calm, non-panic warnings.
- Secure and private communication.
- Authority alerts only when necessary.
- Low-cost and scalable design.

🏁 Conclusion

The **Smart Cooperative Vehicle Warning System** bridges the gap between basic safety systems and expensive autonomous technologies. By combining **embedded sensing, private wireless communication, and human-centric design**, it reduces accidents, improves emergency response time, and enhances overall road safety.

COMMUNICATION SAVE SECONDS

SECONDS SAVE LIVES