International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 15 Issue 3, March-2026

Electric Vehicle Automation and Security Alert System

Navnath S. Govekar[1], Sairaj R Bagal[2], Ketan V Karvande[3], Darshan S Jagadale[4], Pratik D Dalvi[5]

[1]Head of the Department, Department of Electrical Engineering, Navsahyadri Group of Institutions, Pune, Maharashtra, India
[2,3,4,5]Students, Department of Electrical Engineering, Navsahyadri Group of Institutions, Pune, Maharashtra, India

ABSTRACT

The rapid growth of electric vehicles (EVs) marks a major transition in the global automotive industry toward sustainable and energy-efficient transportation. However, the increasing reliance on electronic and networked vehicle systems introduces new challenges related to automation, safety, and security. This paper presents the design and implementation of an Electric Vehicle Automation with Security Alert System, aimed at enhancing driving efficiency, ensuring occupant safety, and preventing unauthorized access or theft. The proposed system integrates several technologies, including microcontroller-based control units, IoT communication modules, and intelligent sensor networks. Vehicle automation functions such as speed regulation, obstacle detection, collision avoidance, and automatic braking are achieved through ultrasonic and infrared sensors interfaced with a central control unit. Battery management and vehicle status are monitored in real time to optimize energy consumption. A key innovation of the system is the security alert mechanism, which employs Global Positioning System (GPS) and Global System for Mobile communication (GSM) technologies to detect abnormal vehicle activity. In the event of unauthorized access or motion, the system automatically transmits a real-time location alert to the owner's mobile device, allowing immediate response and tracking. Furthermore, the vehicle's operational data can be uploaded to a cloud-based server, enabling remote monitoring and control through a mobile or web application. This integration of automation and security not only enhances user convenience but also contributes to the overall reliability and resilience of electric vehicles. The proposed model demonstrates how embedded systems and IoT-based communication can be effectively combined to develop a smart, secure, and eco-friendly transportation platform aligned with the objectives of intelligent mobility and sustainable development.

Keywords - Electric Vehicles (EVs), Vehicle Automation, Embedded Systems, Obstacle Detection, Collision Avoidance, Automatic Braking System, GPS Tracking, GSM Communication, Battery Management System (BMS).

INTRODUCTION

The rapid growth of Electric Vehicles (EVs) has transformed the modern transportation sector by offering a cleaner, more energy-efficient, and sustainable alternative to conventional internal combustion engine vehicles. As EV adoption increases, there is a growing need to integrate advanced automation technologies to enhance vehicle performance, user convenience, safety, and security. Automated systems allow EVs to operate intelligently by monitoring their environment, optimizing energy consumption, and assisting the driver with real-time decision-making. However, along with technological advancement comes the challenge of vehicle security. EVs are particularly vulnerable to risks such as unauthorized access, battery theft, charging port tampering, and system hacking due to their electronic and software-driven architecture. Therefore, incorporating a Security Alert System into EV automation becomes essential to protect both the vehicle and its users. The "Electric Vehicle Automation with Security Alert System" project focuses on designing a smart, automated EV model equipped with sensors, controllers, and communication modules to ensure efficient operation and robust security. Automation functions such as motor control, battery monitoring, obstacle detection, and speed regulation are integrated with security features like intrusion detection, vibration sensing, GPS tracking (if included), and alert notifications through buzzer or wireless communication. By combining automation and security in a single system, the project aims to demonstrate how intelligent technologies can enhance EV reliability, safety, and user trust. This integrated approach provides a foundation for future advancements in autonomous EVs, smart mobility, and safe transportation systems.

LITERATURE SURVEY

1. Scope & method
Focus: research on automation (perception, planning, ADAS/autonomy) for electric vehicles (EVs), together with security safety-alert systems that detect and respond to cyber and physical threats (in-vehicle network attacks, sensor spoofing, EV charging/connected-infrastructure attacks, V2X threats). Sources: recent surveys and domain papers (perception, V2X, IDS, EV reviews, EV charging security).

2. High-level findings (summary)
EVs + Automation are tightly coupled: research increasingly treats electric vehicles as the platform for advanced driver assistance and autonomous features — work covers sensors, control algorithms, and EV-specific constraints (battery, weight, regen braking). Perception is a dominant research area: 2D/3D object detection, sensor fusion (camera, radar, LiDAR, ultrasonic) and real-time perception pipelines are heavily studied because safety depends on reliable perception.

3. Thematic deep dives
3.1 Perception & obstacle avoidance
Topics: 3D object detection, semantic segmentation, sensor fusion, real-time constraints.
Typical approaches: deep learning (point clouds, images), LiDAR+camera fusion, model compression for edge devices.
Key challenges: adverse weather/night, sensor spoofing (e.g. LiDAR laser "ghosts"), low compute budgets.

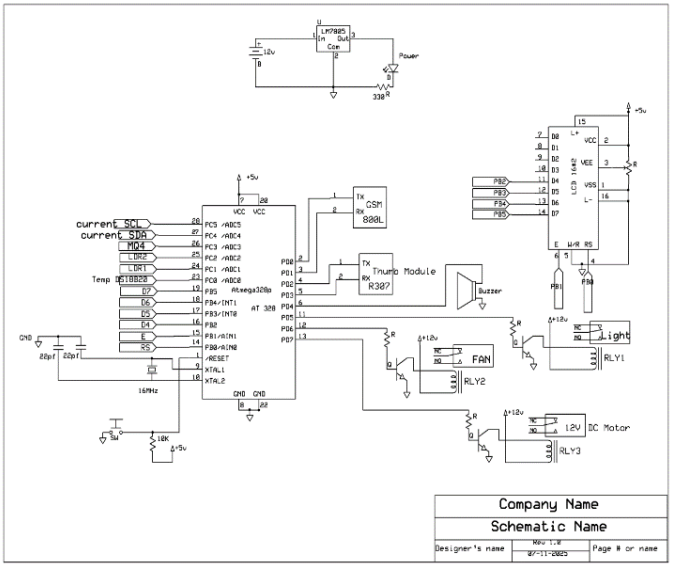
4. Typical attack vectors relevant to an EV automation + alert system
Sensor attacks: LiDAR/radar/camera spoofing and jamming (e.g., laser spoofing creates ghost obstacles). In-vehicle network attacks: malicious messages over CAN/ethernet that influence actuators. V2X message manipulation: false hazard broadcasts or replay attacks. Charging infrastructure compromise: data tampering, denial of service or financial fraud.

5. Datasets, benchmarks & platforms
Datasets for perception (KITTI, nuscenes, Waymo) are widely used for detection and fusion research (see 3D detection surveys). For network security, public CAN datasets are fewer and often not representative of production EVs — a frequently-cited limitation
.

HARDWARE REQUIREMENT

- Microcontroller AT Mega 328
- Regulator LM2596 DC-DC Buck Converter
- Lcd 16*2
- Temp DS18B20 sensor
- MQ4 Sensor
- GSM 800L module
- Relay 1 –Light
- Relay 2– FAN
- Relay 3-12v DC motor
- LDR2
- Buzzer
- Thumb Module R3073
- Current /Voltage INA219 sensor

METHODOLOGY



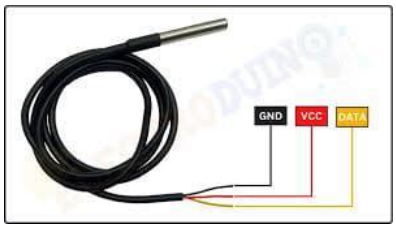
Circuit diagram

This circuit diagram represents a microcontroller-based automation and monitoring system using an ATmega328P microcontroller (commonly used in Arduino Uno boards). It interfaces with sensors, actuators, and communication modules such as GSM and a fingerprint sensor.

- Main Components

1.Power Supply Section
LM7805 voltage regulator: Converts 12 V DC input to a regulated 5 V DC output.
Capacitors (330 Ω resistor, filter caps): Used for voltage stabilization and noise filtering.
Provides both +5 V and +12 V rails for different parts of the circuit.
2.Microcontroller: ATmega328P

3. Sensors Connected
Current Sensor (SCL, SDA) — likely I²C-based current measurement module. LDR (Light Dependent Resistor) — measures ambient light. Temperature Sensor (DS18B20) — measures temperature digitally.



Temperature sensor

These inputs allow environmental and electrical parameter monitoring.

4. Output/Actuator Section
Relay 1 (RLY1): Light Control Drives a 12 V light based on sensor/microcontroller command.
Relay 2 (RLY2): Fan Control
Relay 3 (RLY3): DC Motor Control
Relays are controlled via NPN transistors (switching drivers) connected to ATmega digital pins

5. Communication Modules

GSM Module

GSM Module (SIM800L) Used for sending / receiving SMS or remote monitoring commands.
TX/RX connected to ATmega PD0/PD1 for serial communication. Thumb/Fingerprint Module (R307) Used for biometric access or authentication

6. Display Unit

16×2 LCD Display connected to port PB (PB0–PB5). Displays system status, sensor readings, or alerts.

7. Additional Components
Buzzer for audio alert or indication. Push Button (SW4) for reset or manual input. Pull-up resistor (10 kΩ) on reset line to ensure stable reset behavior.

CONCLUSION

The development of an Electric Vehicle (EV) automation system integrated with a security alert mechanism demonstrates a significant step toward enhancing vehicle safety, efficiency, and user convenience. The project successfully combines sensor-based monitoring, automated control, and real-time locking/unlocking—the system reduces human dependency and minimizes operational risks. alert communication to create a smarter and more secure EV environment. By automating critical functions—such as intrusion detection, battery status monitoring, obstacle sensing, and vehicle

The inclusion of security alerts via buzzer, GSM, IoT dashboard, or mobile notifications ensures timely user awareness, thereby preventing unauthorized access and improving overall vehicle protection. The system's modular design also allows for scalability, enabling future enhancements such as GPS tracking, advanced driver-assistance features, AI-based threat detection, and cloud analytics.

Overall, the project highlights how automation and intelligent security systems can transform electric vehicles into safer, smarter, and more user-centric solutions. It contributes to the growing field of intelligent transportation and sets the foundation for further innovation in EV technology and automotive cyber security.

REFERENCES

[1] S. Sripad, S. Kulandaivel, V. Pande, V. Sekar, and V. Viswanathan, "Vulnerabilities of Electric Vehicle Battery Packs to Cyberattacks."(2017)
[2] C. Douligeris, "Electric vehicle charging: a survey on the security issues and challenges of the open charge point protocol (ocpp)," IEEE Communications Surveys & Tutorials, 2022.
[3] SIMCom,"SIM900AHardwareDesign",Datasheet:https://components101.com/sites/default/files/component_datasheet/SIM900A%20Datasheet.pdf[Last Accessed on 2022 Jan. 7]
[4] Bautista, John Michael, et al. "Real-time vehicle accident alert system based on Arduino with SMS notification." Southeast Asian journal of science and technology 4.1 (2019): 98-100
[5] B. G. Nagaraja, R. Rayappa, M. Mahesh, C. M. Patil, and T. C. Manjunath, "Design & development of a GSM based vehicle theft control system," Proc. -Int. Conf. Adv. Comput. Control. ICACC 2009, pp. 148–152, 2009, doi: 10.1109/ICACC.2009.154.