

DRIVE GUARD-IOV BASED DANGEROUS DRIVING DETECTION AND WARNING SYSTEM

B.Uday prakash¹, B.Lavanya², D.Bhavana³, D.Shilpa⁴, B.Mythily Devi⁵

1 Department of Electronics and communication engineering, Gurunanak InstITutions technical campus, Hyderabad.

ABSTRACT

In this project, proposed a novel driver behavior monitoring and warning (DBMW) framework designed to enhance road safety through the Internet of Vehicles (IoV). The DBMW framework leverages wearable sensing devices to continuously monitor driver head movements and detect behavioral anomalies. According to our literature review, DBMW is the first framework of its kind to offer the following capabilities: Continuous monitoring of driver behavior and real-time measurement of anomaly levels using wearable devices; Immediate transmission of warning messages concerning potentially dangerous driving behaviors to nearby vehicles and pedestrians via IoV communication protocols. This proactive alert system enables surrounding road users to stay informed about high-risk drivers in their vicinity, allowing them to take preventive measures to avoid potential accidents or collisions. To evaluate the practicality and effectiveness of the proposed framework, we implemented a prototype consisting of an Android-based sensing unit and an Arduino-based wearable device. Experimental results demonstrate that DBMW significantly improves detection accuracy and reduces false alarm rates compared to existing methods, offering a robust and scalable solution for intelligent driver behavior analysis and real-time traffic safety enhancement.

The increasing number of road accidents caused by unsafe driving behaviors has become a major concern for transportation systems worldwide. Dangerous driving actions such as overspeeding, sudden braking, harsh acceleration, and lane deviation can lead to serious accidents and loss of life. To address this problem, intelligent technologies are being developed to monitor driver behavior and provide timely warnings to prevent accidents. The Internet of Vehicles (IoV) plays an important role in improving road safety by enabling communication between vehicles, roadside infrastructure, and cloud networks.

The Drive Guard IoV-based dangerous driving detection and warning system is designed to monitor driving behavior in real time and identify risky driving situations. The system uses various sensors installed in the vehicle, such as accelerometers, gyroscopes, and GPS modules, to collect important driving data including vehicle speed, acceleration, braking patterns, and location.

Key words : Aurdino UNO, Accelerometer sensor, Eye blink sensor, Internet of Vehicles.

I.INTRODUCTION

Humans tend to pursue carelessness and try to recover from these mistakes ultimately with the use of technology. Hence, they created cars, Planes etc. just to overcome difficulty of mode of transportation. However, there are some guidelines that need to be abided while taking control of these machines and gaining access to them. The priority of saving drivers and passengers on the road is a n ever growing need in the wake of high number of fatalities caused from road accidents in recent years. Driver drowsiness has been identified as a leading cause of road accidents, identifying the following signs: such as the inability tokeep yourself wide awake, yawning, inability to keep head straight, all those being common indicators of driver fatigue [1]. To overcome this problem, this application focuses on identifying the signs and

tackling driver drowsiness that can be observed on all face shapes while driving and how they can be used to prevent road accidents[10]. Earlier, drowsiness applications were primarily directed towards logistics-based firms such as Amazon in the US. However, many drivers had registered for a complaint about the unauthorized access of their privacy when such monitoring systems were used. As of now, aims to make the overall software less intrusive and a system to monitor eye movements [2]. This allows for a more low-key system for drivers, ensuring that they feel at ease while driving.

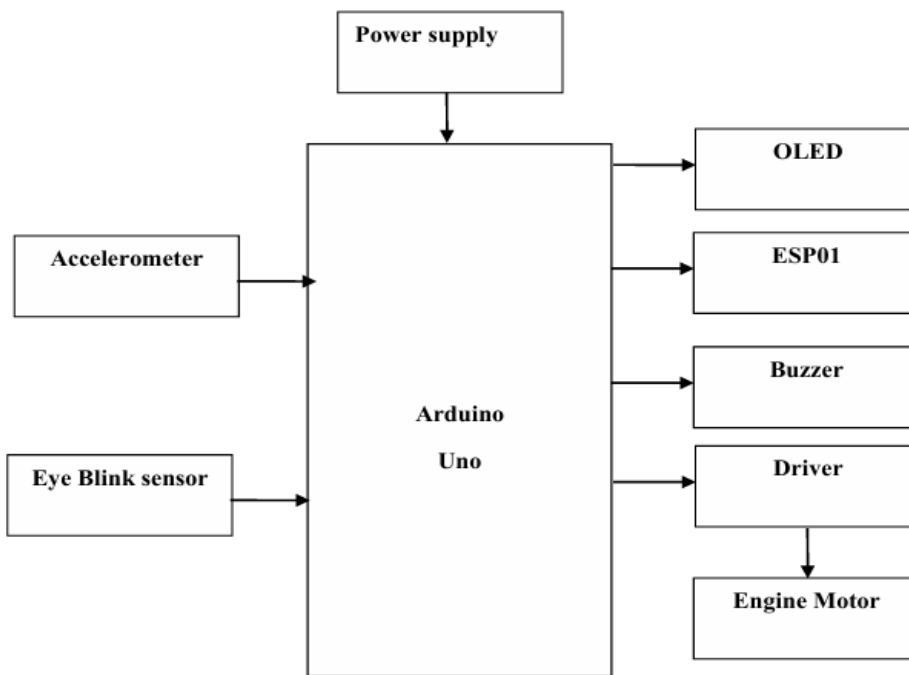
II.PROJECT DESCRIPTION

An embedded system can be defined as a computing device that does a specific focused job. Appliances such as the air-conditioner, VCD player, DVD player, printer, fax machine, mobile phone etc. are examples of embedded systems. Each of these appliances will have a processor and special hardware to meet the specific requirement of the application along with the embedded software that is executed by the processor for meeting that specific requirement. The embedded software is also called “firm ware”. The desktop/laptop computer is a general-purpose computer. You can use it for a variety of applications such as playing games, word processing, accounting, software development and so on. In contrast, the software in the embedded systems is always fixed listed below:

- Embedded systems do a very specific task, they cannot be programmed to do different things.
- Embedded systems have very limited resources, particularly the memory. Generally, they do not have secondary storage devices such as the CDROM or the floppy disk.
- Embedded systems have to work against some deadlines. A specific job has to be completed within a specific time. In some embedded systems, called real-time systems, the deadlines are stringent. Missing a deadline may cause a catastrophe-loss of life or damage to property.
- Embedded systems are constrained for power. As many embedded systems operate through a battery, the power consumption has to be very low.
- Some embedded systems have to operate in extreme environmental conditions such as very high temperatures and humidity.

Traffic accidents are intrinsically unpredictable. Numerous studies investigating traffic accidents have focused on conveying accident information to relevant parties in the shortest time possible and on assisting drivers and injured people as quickly as possible [10], [11]. Several studies have noted that driver behavior is the main factor causing traffic accidents, and therefore, they have used a controller area network (CAN bus) and other sensors to collect vehicle data. Kaplan et al. [12] identified drowsiness and driver distraction as the main reasons for traffic accidents. They proposed a method to monitor a driver’s physical state by using a smartphone and a wearable device as well as to notify other drivers of potential risks through vehicle-to-vehicle (V2V) technology. Jadhav and Wagdarikar [13] used an embedded system to receive data from sensors such as eye-blink sensors, CAN buses, webcams, and GPS receivers. After data analysis, GSM modules transmit the status to a server.

Figure-1

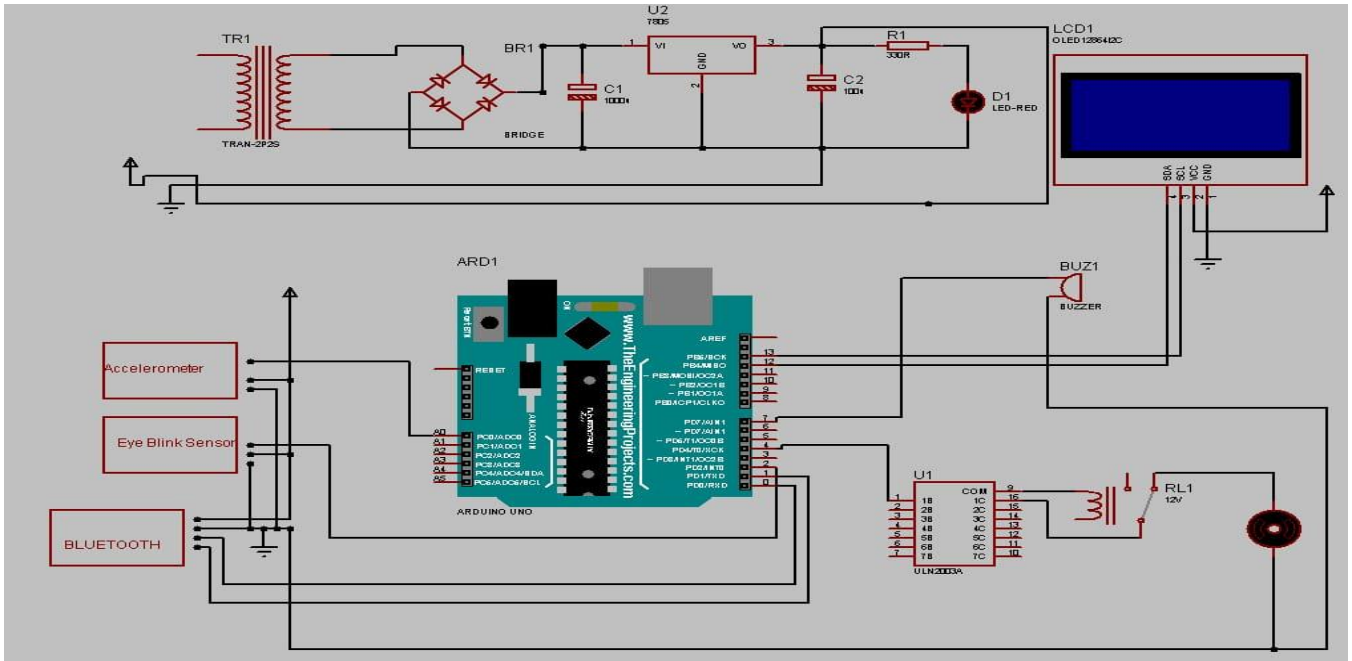


III.FRAMEWORK DESIGN

The core services of the framework proposed herein, shown in Fig. 1, consist of the raw data receiver (RDR), warning area decision service (WADS), accident pattern recognition service (APRS), message generator (MG), and user profile service (UPS). This section discusses the design of these services. Some phenomena are observed from accident data: 1) high-accident-likelihood periods overlap with peak traffic periods; 2) traffic accident hotspots change over time; 3) transportation use differs by age group among the victims of accidents; and 4) the distribution and time occurrence of accident hotspots differ between working days and holidays. As mentioned previously, we propose a framework based on the spatial distribution of traffic accidents. An alert service requires a reaction when an alert has the highest priority, even when the framework is under heavy loading. Therefore, fast computing and transmission are the most critical elements of our framework design. The framework can be divided into five services. five services.

- 1) The RDR is responsible for receiving information from the vehicle—including speed, latitude and longitude, and identity—and forwarding this to the AMQP. The RDR is also responsible for preliminary data filtering. For example, the receiver stops forwarding data when the vehicle’s speed is zero. 2) The WADS determines whether a vehicle has entered the warning area by using the results obtained through DBSCAN. 3) The APRS infers the risk of a traffic violation and alerts drivers according to their time period and location. This service uses the association calculation algorithm to classify historical accident records by applying multiple parameters including a driver’s personal information, date and time, and traffic flow as inputs.
- 2)

Figure-2



The framework design of a Drive Guard IoV-based dangerous driving detection and warning system is built to monitor driving behavior, analyze risks in real time, and provide immediate alerts to drivers and nearby vehicles. The system mainly works through the integration of vehicle sensors, communication networks, data processing units, and warning mechanisms.

In this system, vehicles are equipped with multiple sensors such as accelerometers, GPS modules, cameras, and gyroscopes. These sensors continuously collect data related to vehicle speed, acceleration, braking patterns, lane position, and surrounding traffic conditions. The collected data is transmitted to the onboard processing unit or a connected cloud server through Internet of Vehicles (IoV) communication technologies such as Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I).

The processing unit analyzes the incoming data using predefined rules or machine learning algorithms to identify abnormal or risky driving behaviors. Examples of dangerous driving patterns include sudden braking, rapid acceleration, overspeeding, sharp turns, lane deviation, and driver distraction. The system compares real-time data with safety thresholds to determine whether the driving behavior is safe or potentially dangerous.

When the system detects unsafe driving behavior, it immediately generates warnings. These alerts are delivered through different interfaces such as dashboard notifications, audio alarms, or mobile applications. In some cases, the warning message is also transmitted to nearby vehicles or traffic management systems through IoV communication to prevent possible accidents. The framework also includes a cloud-based data management system that stores driving data for further analysis. This data can be used to improve traffic safety, study driving patterns, and support intelligent transportation systems. Authorities or fleet managers can access the stored information to monitor driver performance and take preventive measures.

Overall, the framework works as an intelligent safety layer for vehicles by combining sensing, communication, data analysis, and alert mechanisms. It helps in early detection of dangerous driving situations and provides timely warnings, thereby reducing the risk of road accidents and improving overall road safety.

IV.FRAMEWORK IMPLEMENTATION AND PROTOTYPE

Framework Implementation and Prototype of Drive Guard IoV-Based Dangerous Driving Detection and Warning System

The implementation of the Drive Guard IoV-based dangerous driving detection and warning system focuses on developing a working model that can collect driving data, detect unsafe driving behavior, and provide warnings in real time. The prototype is designed by integrating hardware components, communication technologies, and software algorithms.

The system is implemented using a set of sensors installed in the vehicle to monitor driving parameters. Sensors such as accelerometers, gyroscopes, and GPS modules are used to collect data related to vehicle speed, acceleration, braking, and location. These sensors continuously send data to a microcontroller or onboard processing unit such as Arduino, Raspberry Pi, or any embedded system. The onboard unit processes the data and identifies abnormal driving patterns.

The prototype system uses Internet of Vehicles (IoV) communication technologies to transmit information between vehicles and external systems. Wireless communication methods such as Wi-Fi, Bluetooth, or cellular networks are used to share driving information. Through Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication, the system can exchange warning messages with nearby vehicles or traffic management systems.

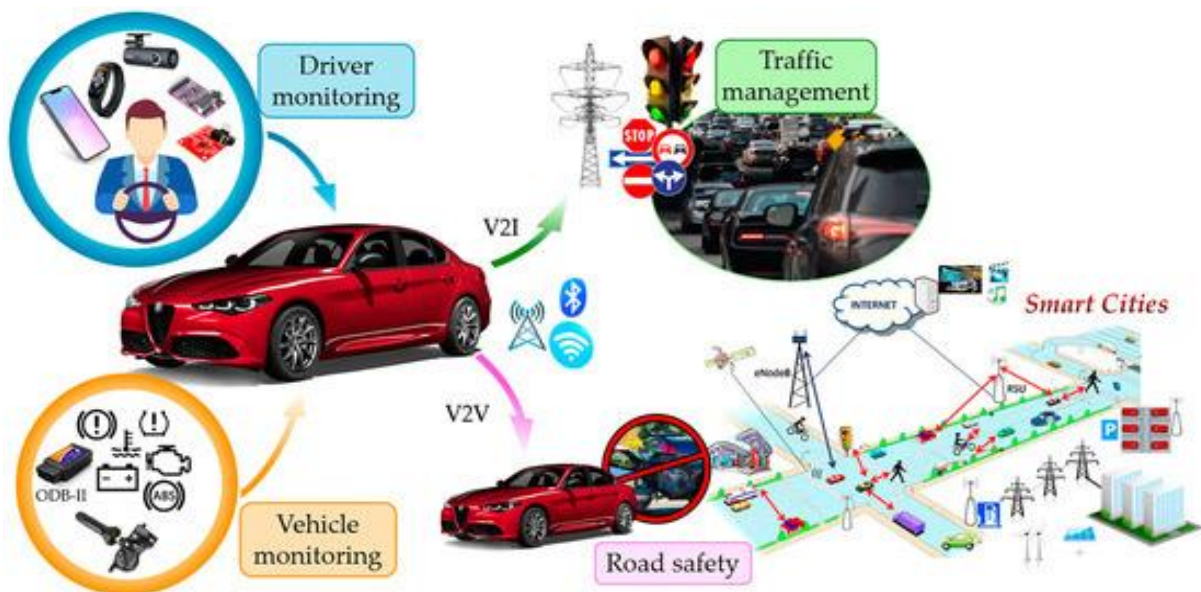
A software module is implemented to analyze the collected sensor data. The system compares the real-time driving data with predefined safety thresholds. For example, sudden braking, excessive speeding, rapid acceleration, or sharp turning may indicate dangerous driving behavior. Machine learning or rule-based algorithms can be used to detect these risky actions.

When the system identifies dangerous driving behavior, it generates warning alerts. These alerts can be displayed on the vehicle dashboard, mobile application, or audio alarm system. The alert mechanism helps the driver immediately become aware of unsafe driving conditions and take corrective actions.

The prototype also includes a cloud or database system to store driving data for future analysis. The stored data can be used to evaluate driver performance, analyze accident patterns, and improve road safety strategies. Fleet managers or traffic authorities can access this information through a monitoring interface.

Overall, the implementation and prototype demonstrate how IoV technology can be used to create an intelligent driving safety system. By combining sensors, communication networks, data processing, and alert systems, the Drive Guard framework effectively detects dangerous driving behavior and provides timely warnings to reduce accidents and improve road safety.

Figure-3



V.CONCLUSION

Drive Guard a real time affordable driver-drowsiness detector has been developed using Kotlin Android Application on the basis of facial behavior such as eye detection and yawn detection by capturing real time facial data. Drive Guards' eye detection technology tracks the movement and behavior of the driver's eyes. The identified facial features on the basis of how prolonged the eye closure is and how erratic the eye movement is, which are clearly indicative of the fatigue. By providing real time monitoring alert, Drive Guard aims to prevent potential accidents. With Kotlin's powerful capabilities and the CNN's facial detection this innovative application offers an effective solution for solution for combating driver drowsiness in real time. The Drive Guard IoV-based dangerous driving detection and warning system provides an intelligent approach to improve road safety by using Internet of Vehicles technology. The system continuously monitors driving behavior through sensors and analyzes data such as speed, acceleration, braking, and lane movement. By processing this information in real time, the system can quickly detect unsafe or risky driving patterns.

When dangerous driving behavior is identified, the system immediately generates warning alerts to the driver through dashboard notifications, audio alarms, or mobile applications. At the same time, IoV communication allows the system to share warning messages with nearby vehicles and traffic infrastructure, helping other drivers become aware of potential hazards.

The integration of sensing technologies, onboard processing, wireless communication, and cloud storage makes the system efficient and reliable for detecting risky situations. The stored data can also be used for traffic analysis, driver behavior evaluation, and improving intelligent transportation systems.

VI.REFERENCE

- 1 Thomas, R. M., & Divya, S. B. (2019). An Intelligent Application for Detecting and Alerting on Dangerous Driving Behaviors. *International Journal of Engineering Research & Technology (IJERT)*.
- 2 He, J., Zhong, K., Wu, S., & Liu, P. (2022). Research on Dangerous Driving Behavior Detection Based on YOLOv5 Algorithm. *Science Discovery Journal*.
- 3 Sun, S., Bi, J., Guillen, M., & Pérez■Marín, A. (2020). Assessing Driving Risk Using Internet of Vehicles Data. *Sensors Journal (MDPI)*.
- 4 Li, B., Li, E., & Li, H. (2021). Aggressive Driving Detection and Alert System Using Smartphone Sensors. *Journal of Student Research*.
- 5 Ferreira, L., Valente, A., & Salgado, P. (2023). Advances on Risky Driver Behaviour Detection in Road Vehicles. *Artificial Intelligence Review*.
- 6 Zhang, Y., Wang, H., & Liu, J. (2021). Driver Behavior Monitoring and Warning System Based on Internet of Vehicles. *IEEE Conference Proceedings*.
- 7 Chen, X., Xu, Z., & Wang, L. (2020). IoT-Based Smart Vehicle Monitoring System for Dangerous Driving Detection. *International Journal of Advanced Computer Science*.
- 8 Kumar, P., Singh, R., & Sharma, A. (2022). Intelligent Transportation System for Detecting Dangerous Driving Patterns Using Machine Learning. *International Journal of Intelligent Transportation Systems*.
- 9 Patel, D., Shah, N., & Mehta, R. (2021). Real-Time Vehicle Monitoring and Accident Prevention System Using IoT. *International Journal of Engineering and Technology*.
- 10 Gupta, S., Verma, P., & Singh, K. (2023). Smart IoV Framework for Driver Safety and Traffic monitoring. *Journal of smart transportation*