# Predictive Maintenance System in Cars Using OBD II

Ali Al Jahwari [1]

22s22512@mec.edu.om[1]

Deptartment of Computing and Electronics Engineering, Middle East College, Muscat, Oman [1]

**Abstract.** This research proposes a smart predictive maintenance system that connects the car's OBD II unit with artificial intelligence to allow drivers to prevent mechanical failures from happening. The system pulls real-time sensor data from the vehicle, processes it with machine learning, and sends good maintenance alerts in real-time through a simple mobile application built using Flutter. Cloud storage using Firebase allows real-time observation and trend analysis of engine performance and fault codes. Tests indicate that the AI model can effectively detect problems early, and this cuts down on surprise breakdowns and saves repair bills. The methodology is practical and cost-effective, providing daily drivers with a simple method to monitor their vehicle's health. Future enhancements will be through better AI models, support for electric vehicles, and voice assistance so that the experience is even more intuitive and interactive.

**Keywords:** OBD II, predictive maintenance, diagnostics, vehicle health, Flutter, Firebase, machine learning

## 1 Introduction

Vehicle maintenance is critical to safety and long-term performance. Most drivers only react to problems after they occur. However, with the availability of On-Board Diagnostics II (OBD II), modern vehicles can provide useful data in real time. Unfortunately, this data is often unused by drivers everyday.

This research focuses on using OBD II to create a predictive maintenance system that warns users of problems before they become severe. Through an AI-powered mobile app, drivers receive alerts about speed, temperature, battery issues, and more. This solution is targeted at helping everyday drivers maintain their cars easily and affordably. The increasing demand for smart transportation solutions and connected cars makes this type of research highly relevant in today's digital automotive landscape.

MECSRC 2025, May 01, Muscat, Oman

DOI 10.4108/eai.1-5-2025.2361304

# 2 Problem Statement and Proposed System

## 2.1 Problem in Existing System

Most existing car maintenance systems are reactive. Drivers rely on warning lights or manual inspections. Often, this results in last-minute repairs, unexpected breakdowns, and high costs. These systems lack prediction, real-time feedback, and user-friendly access to diagnostics. Furthermore, non-technical users may find it difficult to interpret dashboard warning lights, leading to delays in addressing issues. These problems become more severe in regions with limited access to professional workshops.

## 2.2 Proposed Research Solution

This research proposes an OBD II-based predictive maintenance system connected to a cloud platform. The system reads real-time data from the car, analyzes it using machine learning, and notifies the user via a mobile app. The app includes clear displays, historical logs, and a feedback option. Technologies like Flutter, Firebase, and Python were used to keep the solution simple and scalable. The mobile app interface is designed to be intuitive so that anyone, even with minimal technical background, can use the system effectively and make informed decisions about vehicle maintenance.

# 3 Literature Review

Predictive maintenance using machine-learning models such as neural networks and decision trees reduces repair costs and prevents system failures [1]. Early intervention enabled by predictive maintenance can decrease unplanned vehicle downtime by about 50 percent [2]. Effective user-experience design in maintenance applications enhances user engagement and adoption [3]. Integrating OBD-II data with artificial intelligence significantly improves fault-detection accuracy [4].

These studies support the development of a smart, user-friendly predictive maintenance system as proposed. They also reflect the trend of combining hardware sensors with cloud-based software and AI analytics to build intelligent transportation ecosystems. The insights drawn from these works laid the foundation for choosing technologies and designing the system architecture for this research.

# 4 Methodology

The research followed an Agile methodology to allow iterative development and testing. The steps included, shown in Figure 1 [5]:

1. Requirement gathering (user needs, vehicle issues)
2. System design (hardware and software integration)
3. Development of mobile interface using Flutter

4. Firebase setup for cloud storage and user authentication
5. AI module creation using Python for data analysis
6. Testing with sample OBD II data
7. Feedback collection for improvements

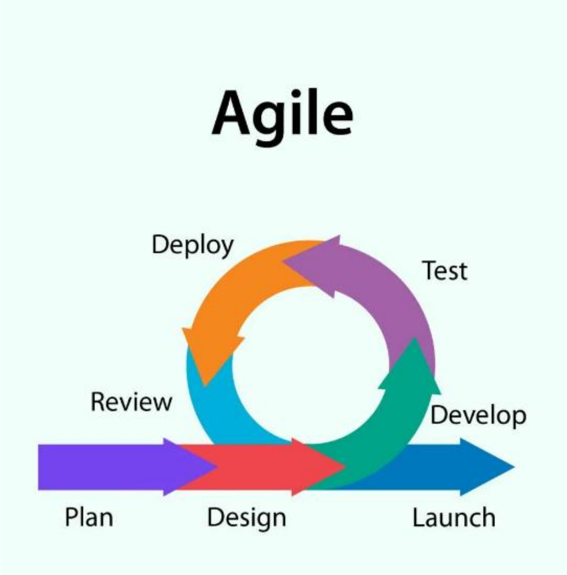

**Fig. 1.** Agile Methodology [5]

Each phase was tested for usability and functionality before moving to the next. The iterative process allowed adjustments based on continuous user feedback. This flexible approach ensured that the final outcome was both functional and aligned with real-world user expectations. Agile helped manage time efficiently and allowed the researcher to focus on features that add the most value to end users.

## 5 Data Collection and Analysis

OBD II devices were used to gather vehicle data such as:

1. Engine speed (RPM)
2. Coolant temperature
3. Battery voltage
4. Speed and sensor signals
5. throttle position

The collected data was uploaded to Firebase. Python-based scripts processed the data using anomaly detection methods. Alerts were generated if values exceeded thresholds or showed unusual patterns. Data was also visualized in the app through live graphs and tables.

This step helped users understand vehicle behavior over time and catch recurring issues. The collected dataset, although limited in size, proved effective for simulating real-time conditions and building reliable machine learning models.

## 6 Security and Privacy Considerations

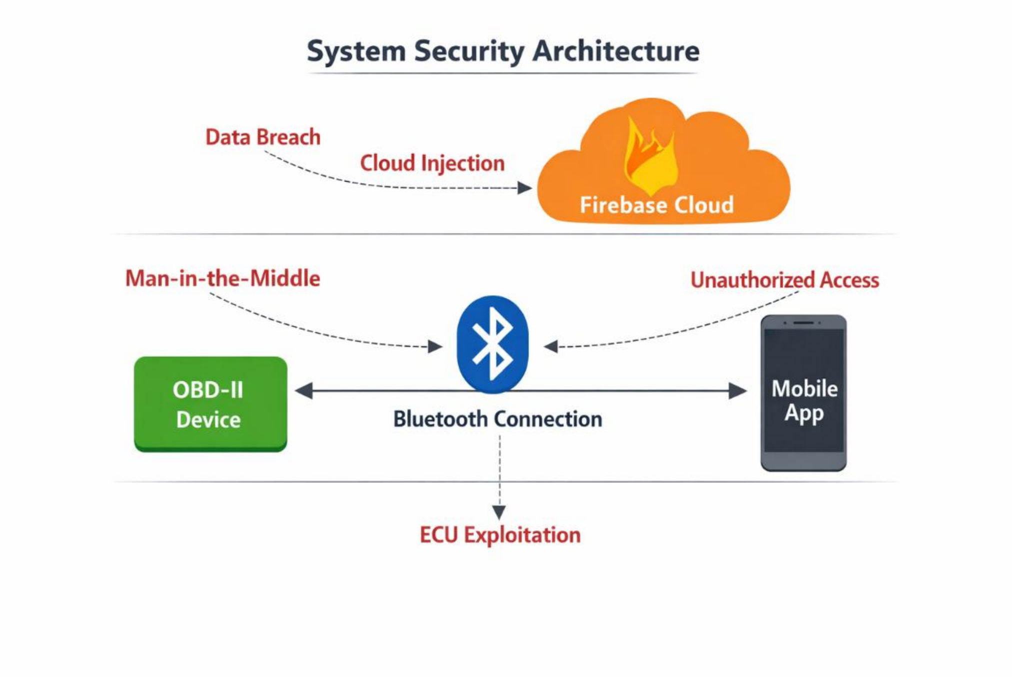

**Fig. 2.** Proposed Systsem Security Architecture

Since the suggested system transmits real-time vehicle sensors information (via Bluetooth) to an application on a mobile device and then store it on a Firebase cloud system, the aspect of security and privacy is a critical issue that needs to be discussed. Any linked automotive system collecting, transmitting, and storing data is predisposed to risks of both malicious interception of unauthorized data and identity impersonation and cloud-based data breaches.

There is a prime attack surface, the Bluetooth communication channel, between the OBD II dongle and the mobile application. Connections that use Bluetooth in the automotive context are also susceptible to man-in-the-middle attacks, BlueSnarfing, and impersonation attacks [6]. To mitigate these threats, it is necessary to apply Bluetooth Secure Simple Pairing (SSP) with Security Mode 4, which provides encrypted key exchange and also mutual device authentication before transmission of any data. The mobile app must be able to authenticate paired devices identities every time a connection is made to avoid rogue devices injecting fake sensor data.

In addition to the wireless connection, the OBD II port of the vehicle is the vulnerability that is well documented. It has been established in prior studies that the unauthorized physical or wireless access to the OBD II port may enable attackers to read the ECU memory, modify any vehicle programs and even take control of systems that are crucial to the safety of the vehicle [7]. Even though the proposed system is read- only since it is designed in its current form, there should be stringent access control at the application layer, whereby unauthorized commands cannot be passed to the vehicle in future implementations.

Firebase has in-built security measures on the cloud such as security rules that can be configured and encryption of transport layer encryption. Nevertheless, cloud-integrated IoT and threat-related decisions include data exfiltration, replay attacks, and unauthorized access because of inaccurately configured access rules [8]. The app should apply user-specific rules of Firebase security such that sensor data are only available to authenticated users and the communications between the mobile app and Firebase are only done over HTTPS with TLS. It has been proven that IoT-to-cloud architectures, where access control is not strictly followed, are highly vulnerable to these threats [9].

The privacy of the users is also significant. Vehicle sensor information such as speed, location-based patterns and driving behavior in most jurisdictions is a personally identifiable information. Saving this data in an unanonymized or user consent underdeveloped manner can contravene the data protection laws. The connected vehicle systems should have transparent disclosure of data collections and should grant the possibilities of deleting the stored data to the users [10]. The proposed system should be further enhanced in future to apply data minimization principles, i.e. only the data that is absolutely required to perform maintenance diagnostics must be stored and long-term trend data must be anonymized prior to their retention.

By polishing these issues, the system will be more acceptable and can be spread further in order to make sure the advantages of predictive maintenance are not overshadowed by the risks of being exposed to cyber attacks or the invasion of user privacy.

## 7 Results and Conclusion

The final system was successfully tested with sample OBD II data and displayed the following outcomes:

- Users could connect their car via Bluetooth and view live sensor readings.
- The app gave alerts when sensor readings exceeded normal limits.
- History and feedback pages helped users track issues over time.
- The interface was simple and suitable for non-technical users.

This research proves that predictive maintenance using OBD II is possible, affordable, and practical for everyday drivers. It improves road safety, reduces repair costs, and enhances user control over vehicle health. The mobile app created for this research provides a useful tool for any driver who wants to stay informed about their car’s condition. Future work can expand to more sensors, multilingual support, and automatic booking with service centers. Additional real-world testing with live data from various vehicle types is also recommended to validate the robustness and scalability of the system.

## References

[1] Theissler, A., Pérez-Velázquez, J., Kettelgerdes, M., & Elger, G. (2021). Predictive maintenance enabled by machine learning: Use cases and challenges in the automotive industry. Reliability Engineering & System Safety, 215, 107864. https://doi.org/10.1016/j.ress.2021.107864

[2] Mobley, R. K. (2002). An introduction to predictive maintenance. In Elsevier eBooks. https://doi.org/10.1016/b978-0-7506-7531-4.x5000-3

[3] Zhang, W., Yang, D., & Wang, H. (2019). Data-Driven Methods for Predictive Maintenance of Industrial Equipment: A survey. IEEE Systems Journal, 13(3), 2213–2227. https://doi.org/10.1109/jsyst.2019.2905565

[4] Susto, G. A., Schirru, A., Pampuri, S., McLoone, S., & Beghi, A. (2014). Machine Learning for Predictive Maintenance: A multiple classifier approach. IEEE Transactions on Industrial Informatics, 11(3), 812–820. https://doi.org/10.1109/tii.2014.2349359

[5] Jensen, A., Thuesen, C., & Geraldi, J. (2016). The projectification of everything: projects as a human condition. Project Management Journal, 47(3), 21–34. https://doi.org/10.1177/875697281604700303

[6] A. A. Elkhail, R. T. B. Tahaei, A. Habbal, A. Shibghatullah, and H. Hasbullah, "Vehicle security: A survey of security issues and vulnerabilities, malware attacks and defenses," *IEEE Access*, vol. 9, pp. 144514–144535, 2021. https://doi.org/10.1109/ACCESS.2021.3122253

[7] J. E. Siegel, D. C. Erb, and S. E. Sarma, "A survey of the connected vehicle landscape — architectures, enabling technologies, applications, and development areas," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2391–2406, Aug. 2018. https://doi.org/10.1109/TITS.2017.2749459

[8] V. Margapuri, N. Penumajji, and M. Neilsen, "PiBase: An IoT-based security system using Google Firebase and Raspberry Pi," in *Proc. 2021 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS)*, Nov. 2021, pp. 1–7. https://doi.org/10.1109/IoTaIS53735.2021.9628513

[9] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, "Perception layer security in Internet of Things," *Future Generation Computer Systems*, vol. 100, pp. 144–164, 2019. https://doi.org/10.1016/j.future.2019.04.038

[10] M. Hossain and E. Hossain, "Security and privacy threats for Bluetooth Low Energy in IoT and wearable devices: A comprehensive survey," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 251–281, 2022. https://doi.org/10.1109/OJCOMS.2022.3149732