

# **ASSIGNMENT 1**

## **IMPORTANCE, IMPACT, FUTURE SCOPE**

**23/09/2022**

### **CYBER ATTACK DETECTION OF ELECTRIC VEHICLES USING PHYSICS GUIDED MACHINE LEARNING**

## **1 IMPORTANCE**

Cyberattacks are becoming common nowadays they are increasing prominently. So our physics guided machine learning model can help to determine cyberthreat in the electric vehicles (EVs). Motivation of this project was from the issues mechanical engineers were facing during investigating the vehicle problems. To protect vehicles from cyberattack use of machine learning technique is required. This technique is efficient which finds fault with high accuracy.

## **2 IMPACT**

Various attacks can harm IOT-enabled system in vehicles. This can lead to danger of vehicles security. Strategy used by machine learning technique can prevent from this type of attacks. This technique can impact on all types of vehicles and calculate the amount of risk and virus present in the machine system.

## **3 FUTURE SCOPE**

This project has vast scope in future we can add additional features to the program and make it more efficient. In the developing era of automation industry. The machine algorithm technique proposed can predict attacks at early stage from getting it to more severe. Vehicles will be more secured with high security as frequently we check the performance of vehicles it will be safe and protected from external virus attacks.

Guide,  
Prof. D. M. Padulkar  
Dept. of AI & DS

Student,  
Yashraj Devrat  
TE(AI & DS ) Roll No. 2237031