**Intrusion Detection System for Internet of Vehicles using Optimized CNN**

*Submitting in partial fulfillment of the requirements for the degree of*

**Master of Computer Applications**

*By*

**MOHAMED FAHEEJ N (23MCA0028)**

**MUDASSIR KHAN G (23MCA0056)**

**JASHWANTH KUMAR S (23MCA0076)**

***Under the guidance of***

**Dr. Jayalakshmi.P**

**Associate professor Sr. Grade 2, SCORE**

**School of Computer Science Engineering and Information Systems**

**VIT, Vellore**

**WINTER SEMESTER – 2023 - 24**



**ABSTRACT :**

In this modern world, there are many new technologies evolving, and in the same way, Cyber-attacks are also following up. Modern vehicles, including Electric vehicles, autonomous vehicles, and connected vehicles, are increasingly connected to the external world, which enables various functionalities and services. These built-in technologies in vehicles help cyber attackers to attack the Internet of Vehicles (IoV), causing vulnerabilities to cyber threats. Due to the need for more security and encryption performance in vehicular networks, Intrusion Detection Systems (IDSs) are a much-needed strategy to protect modern vehicle systems from cyber threats. In this paper, we are proposing the use of Transfer Learning with Machine Learning (ML) and ensemble learning-based IDS for IoV using Recurrent Neural Network (RNN) and some hyper-parameter optimization techniques. The Car Hacking dataset and the CICIDS2017 dataset are used here. This will demonstrate the effectiveness of the proposed IDS for Cyber-attack detection in both intra and external vehicular networks.

**WORK PLAN:**

