NARASARAOPETA ENGINEERING COLLEGE (AUTONOMOUS)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

(2021-2025)

Batch Number	AB8
Team Members	Shaik Yalavarthi Ijaz Ahamad(21471A0557), Sinde Venkata Saptha Girish(21471A0558), Tammisetti Nagendra Babu(21471A0537)
Guide	Dodda Venkatareddy ,Assistant professor
Title	Adaptive Intrusion Detection in CAN-Based Vehicular Networks Using Transfer Learning for Evolving Threats
Domain/Technology	TRANSFER LEARNING
Base Paper Link	https://ieeexplore.ieee.org/document/10808423
Dataset Link	https://ocslab.hksecurity.net/Datasets/car-hacking-dataset
Software Requirements	Browser: Any latest browser like Chrome Operating System: Windows 8 Server or later Programming Language: Python
Hardware Requirements	Processor: Intel Core i5 or above RAM: 8 GB
Abstract	The CAN-based system security is constantly under serious threats due to increasing vehicular network connectivity through sophisticated cyber-attacks. In this paper, we propose an online reconfigurable IDS that uses Transfer Learning (TL) methods to adapt to new attack patterns with minimal retraining. This approach allows refining pretrained models on a specialized car hacking dataset to detect most known and new attacks efficiently, ensuring high detection accuracy while keeping computation costs low. Dynamic reconfigurability assures protection in an ever-evolving threat landscape. Extensive experiments on real-world CAN datasets validate the effectiveness of the proposed approach, achieving an overall detection rate of over 99% for different attack classes. This work demonstrates the potential of TL in enhancing adaptability, efficiency, and accuracy in improving connected vehicle IDSs, providing a robust solution to secure automotive systems against emerging cyber threats.

Signature of the student(s)   **Signature of the Guide**   **Signature of the project coordinator**