Tree-based Intelligent Intrusion Detection System in Internet of Vehicles

The use of autonomous vehicles (AVs) is a promising technology in Intelligent Transportation Systems (ITSs) to improve safety and driving efficiency. Vehicle-to-everything (V2X) technology enables communication among vehicles and other infrastructures. However, AVs and Internet of Vehicles (IoV) are vulnerable to different types of cyber-attacks such as denial of service, spoofing, and sniffing attacks. In this paper, an intelligent intrusion detection system (IDS) is proposed based on tree-structure machine learning models. The results from the implementation of the proposed intrusion detection system on standard data sets indicate that the system has the ability to identify various cyber-attacks in the AV networks. Furthermore, the proposed ensemble learning and feature selection approaches enable the proposed system to achieve high detection rate and low computational cost simultaneously

They have some limitation less number of attack they detected like denial of service, spoofing, and sniffing attacks.and some research gap

We are expansion of attack detection in hybrid ids model:

- we are getting solution for the problem of facing there challenges related to the sophisticated cyber attack threat like ransomware , zero day vuln and side-channel attack
- the traditional ids has not that much accuracy in detection these threats and providing real time threat response

we are covering these points in the project

we will be expanding the threat detection coverage we will work on to overcome the high false positive rates to enhances the accuracy of detection of intrusions

because there are very few work has been done in this hybrid model most work in traditional one only

less work using ai techniques in hybrid model this we will try to achieve in our project to learn and adapt with new attacks

Implementation of hybrid ids

tools & frameworks:

- snort /suricate : for signature based ids
- zeek for both signature &anomaly detection
- Net-flow or pcap for capturing network traffic
- for anomaly detection : ELK stack to collect , process &visualize data

Data collection :

- network traffic logs : wireshark , tcpdump
- system logs: servers , application logs , os logs
- host &network Monitoring : cpu usage , disk space