PROJECT OVERVIEW	**Project Name:** **An Intelligent Data-Driven Model to Secure Intravehicle Communications Based on Machine Learning**	**Project Manager : Sairam Kodimella**

Research Question(s):

In comparison to traditional methods such as AES encryption and the CONTROLLER AREA NETWORK (CAN) protocol, how effective is the implementation of machine learning algorithms in preventing malicious intruder attacks on the communication between sensors and Electronic Control Units (ECU) in electric vehicles?

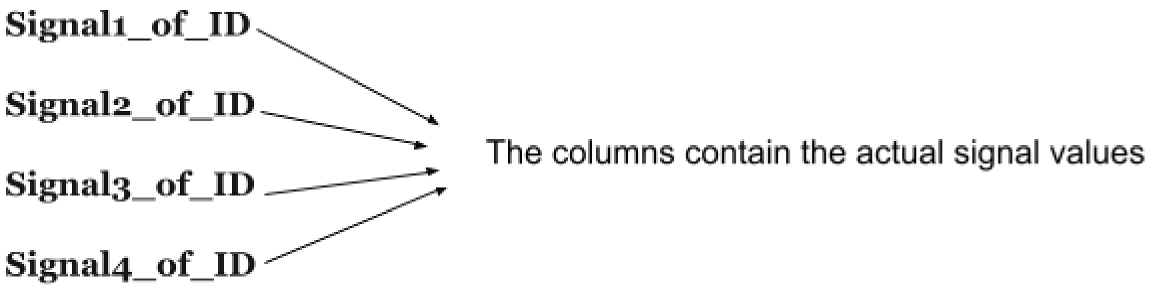
Dataset:

The purpose of this dataset, which we name SynCAN Dataset (Synthetic CAN Bus Data), is to offer a baseline for evaluating and comparing different CAN Intrusion Detection Systems (IDS) on diverse signal space assault scenarios.
The data set consists of a training data set and test data sets that all contain the following columns:

Label - The column 'Label' indicates whether the data row is to be considered as normal (Label=0) or as intrusion (Label=1).

ID - The column 'ID' contains the identifiers for the IDs that are 'id1', ..., 'id10'.

Time - In the column 'Time' the time stamp of the current message is represented in milliseconds.



Signal1_of_ID

Signal2_of_ID

Signal3_of_ID

Signal4_of_ID

The columns contain the actual signal values

Goal:

- Develop an intelligent model that can analyze and monitor intravehicle communications in real-time using machine learning algorithms.
- Identify potential security vulnerabilities and threats in intravehicle communications and develop appropriate countermeasures to prevent attacks.
- Evaluate the performance of the proposed model by comparing it with existing intrusion detection systems in terms of accuracy, speed, and reliability.
- Optimize the model to ensure minimal false positive and false negative rates to prevent unnecessary alarms or missed security threats.
- integrate the model with existing vehicle systems to provide a comprehensive security solution for intravehicle communications.
- Explore the applicability of the model in different types of vehicles, such as passenger cars, commercial vehicles, and autonomous vehicles.

Objectives:

to investigate whether machine learning algorithms are more effective than traditional techniques at stopping hostile intruder attacks.

Success Criteria:

The research's success will depend on whether machine learning algorithms can more accurately, efficiently, and robustly avoid hostile attacks on communication between sensors and Electronic Control Units in electric vehicles than conventional methods can.

Assumptions, Risks, Obstacles:

- The proposed model assumes that sufficient data can be collected and labeled to train the machine learning algorithms.
- The model assumes that the communication protocols used in intravehicle communication are well-defined and can be accurately modeled.
- There is a risk that the model may generate false positives or false negatives, which could result in unnecessary alarms or missed security threats.
- There is a risk that the proposed security measures may not be able to prevent sophisticated attacks that exploit unknown vulnerabilities.
- The lack of standardized communication protocols across different types of vehicles could hinder the development and implementation of the proposed model.
- The collection and labeling of sufficient data for training the machine learning algorithms may be a time-consuming and costly process.

Prepared By	Date	Approved By	Date
Sairam kodimella	FEB14th		