INTRUSION DETECTION SYSTEM

Abhimanyu Tripathi (B222003)
Anshuman Mahabhoi (B422010)
Saumyajeet Varma (B522053)

Under the supervision of
Dr. Puspanjali Mohapatra

INTRODUCTION

- Modern vehicles have evolved into complex cyber-physical systems that rely on thousands of real-time messages exchanged through the **Controller Area Network** (CAN bus).
- The CAN bus is responsible for coordinating critical functions such as braking, steering, engine control, airbags, sensors, and safety mechanisms.
- However, the CAN protocol **doesn’t** includes **authentication**, **encryption**, and **sender verification**.
- This creates major security risks like **DoS attacks**, **Fuzzy attacks**, and **Spoofing attacks**.

MOTIVATION

Intelligent Transportation Growth

Modern vehicles are complex cyber-physical systems. Autonomous cars rely heavily on secure CAN communication.

CAN Protocol Vulnerabilities

Lack of authentication and encryption. Broadcast nature allows injection and flooding attacks.

Inadequacy of Current IDS

Rule-based systems fail against evolving attacks. Existing models suffer from high false-positive rates.

OBJECTIVE

Strengthen Security

Enable early detection of malicious behaviors to support secure transportation ecosystems.

Address CAN Vulnerabilities

Investigate weaknesses like Spoofing and DoS, proposing mechanisms to detect abnormal traffic.

Data-Driven Detection

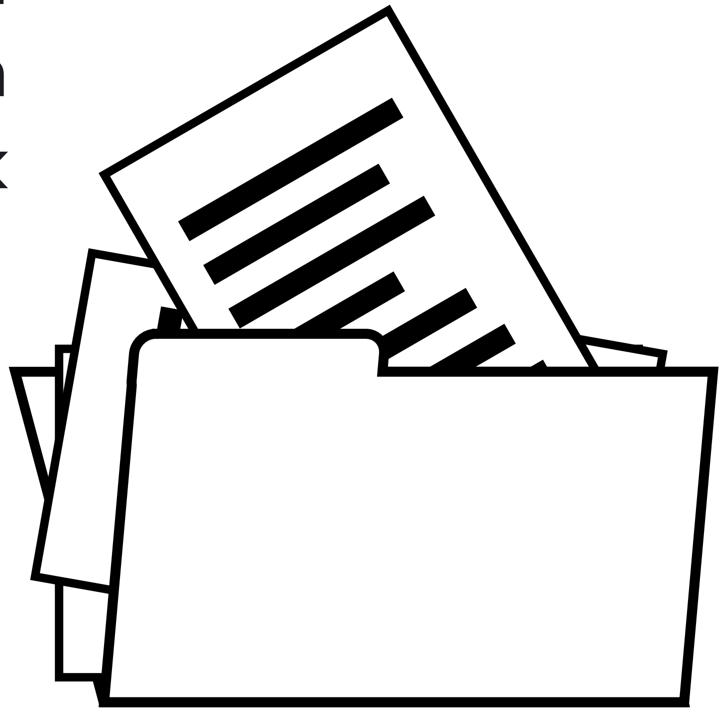
Utilize Machine Learning to model real-world patterns rather than relying on handcrafted rules.

LITERATURE SURVEY OVERVIEW

01: MAFSIDS - A Reinforcement Learning-Based Intrusion Detection Model

MAFSIDS is an intrusion detection framework that combines graph-based deep learning with reinforcement learning to achieve efficient feature selection and high classification performance on large-scale intrusion datasets. The central idea of this work is to reduce redundant features through intelligent selection while maintaining strong detection accuracy across diverse network attack types.

Limitation: The model is computationally expensive due to the use of multiple RL agents and GCN training, is highly sensitive to the design of predefined reward signals, and requires extensive tuning when applied to datasets with different feature distributions.

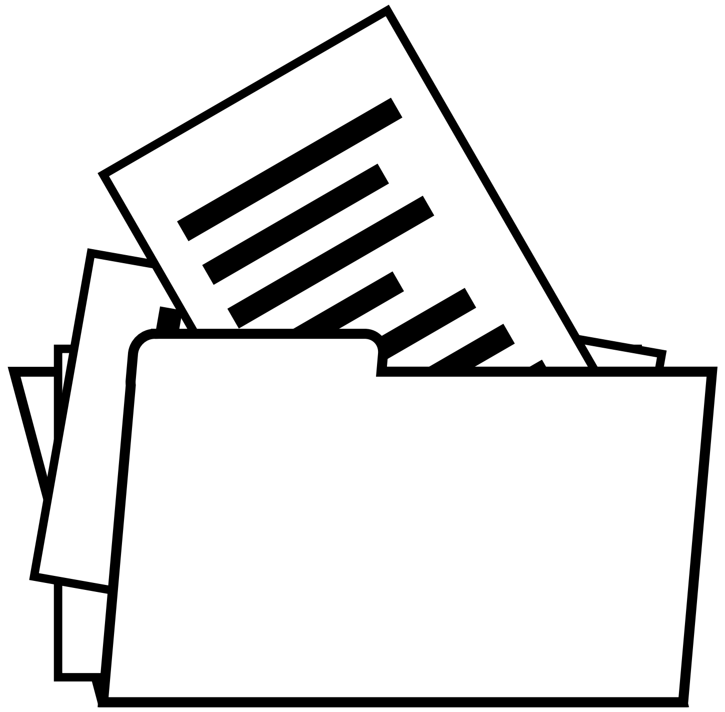


LITERATURE SURVEY OVERVIEW

02: ID-RDRL - Recursive Deep Reinforcement Learning for Intrusion Detection

ID-RDRL aims to enhance intrusion detection by framing feature selection as a learning problem, enabling the system to recursively identify the most informative subset of attributes. This is intended to improve classification quality while reducing computational overhead in handling large feature spaces.

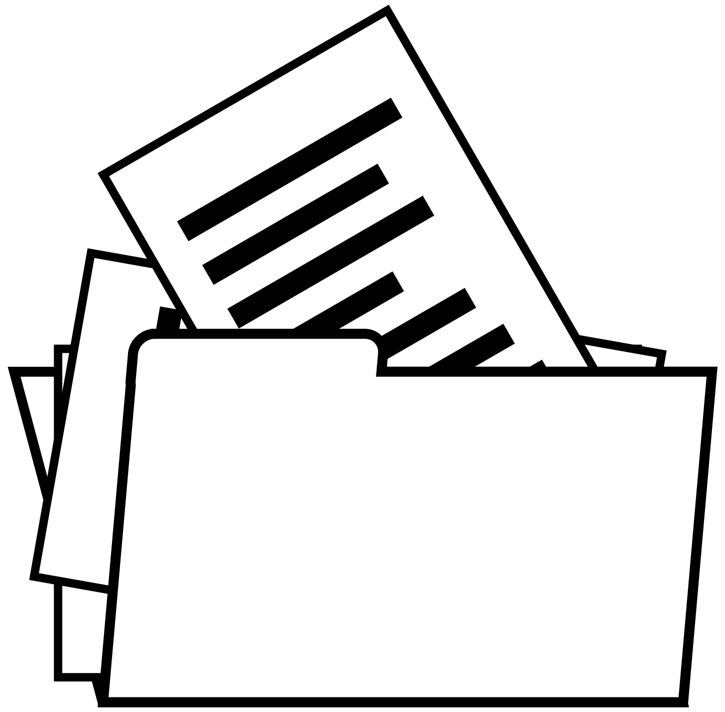
Limitation: The model has a high training cost due to repeated evaluations during the RL-based elimination process, and its performance is strongly dependent on the reward formulation and the choice of base learner in RFE.



LITERATURE SURVEY OVERVIEW

03: Deep Reinforcement Learning IDS Using CIC-IDS2017
This work employs deep reinforcement learning to build an adaptive intrusion detection system capable of handling dynamic and evolving network threats. The study uses the CIC-IDS2017 dataset, which offers realistic and diverse network traffic patterns.

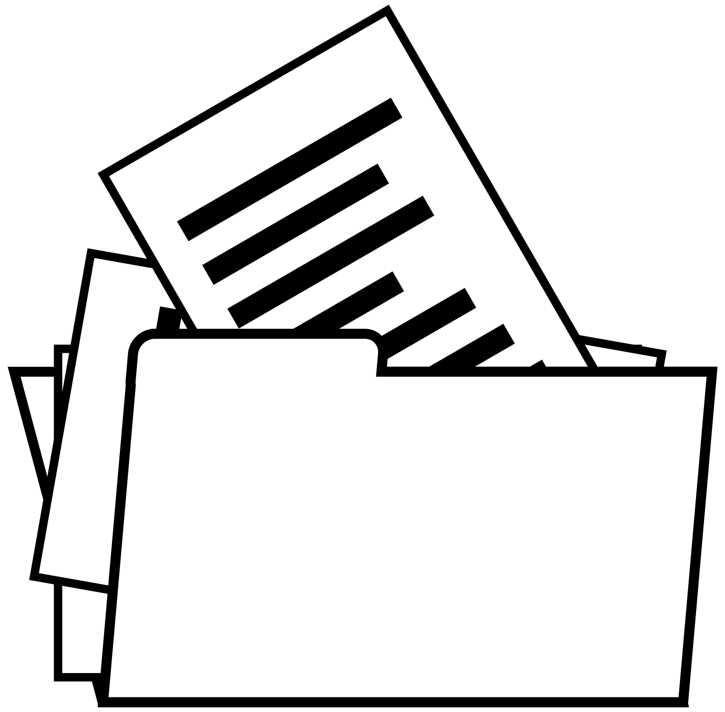
Limitation: A major limitation is the potential for unstable learning when the reward structure is not well-designed, and the model's performance depends heavily on constructing effective state representations, which becomes difficult in complex traffic scenarios.



LITERATURE SURVEY OVERVIEW

04: XGBoost-Based Feature Selection for UNSW-NB15
This study investigates how feature selection based on XGBoost can improve the efficiency and performance of traditional machine learning models on the UNSW-NB15 dataset.

Limitation: Reliance on XGBoost's importance scoring may lead to the removal of subtle features that contribute to non-linear patterns. The approach may not generalize equally well across all classifiers.

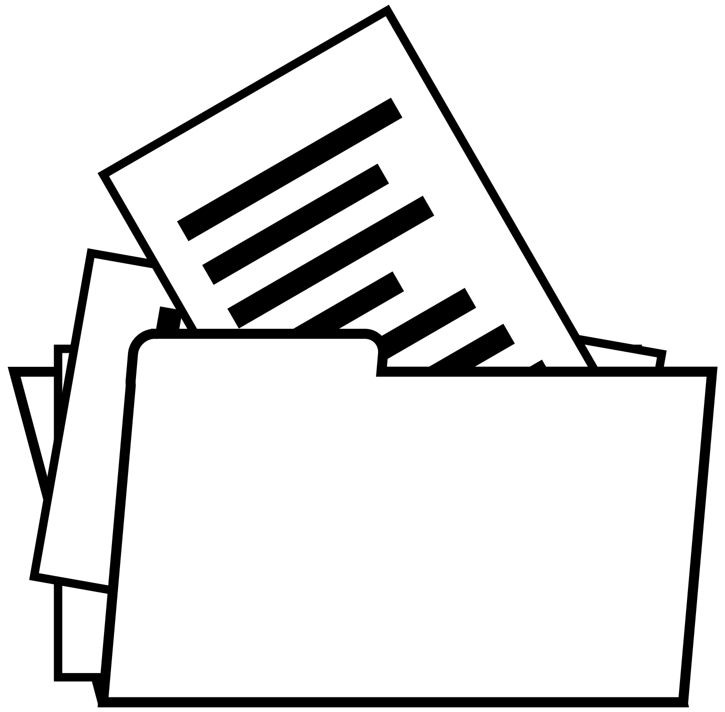


LITERATURE SURVEY OVERVIEW

05: Zero-Day Detection Using Autoencoder-Based Hybrid Models

This research focuses on identifying unknown attacks using anomaly detection techniques that rely on autoencoder reconstruction behavior, combined with supervised learning classifiers

Limitation: Autoencoders may reconstruct malicious patterns too accurately, reducing anomaly detection sensitivity, and their performance is highly dependent on the quality and cleanliness of benign training data.

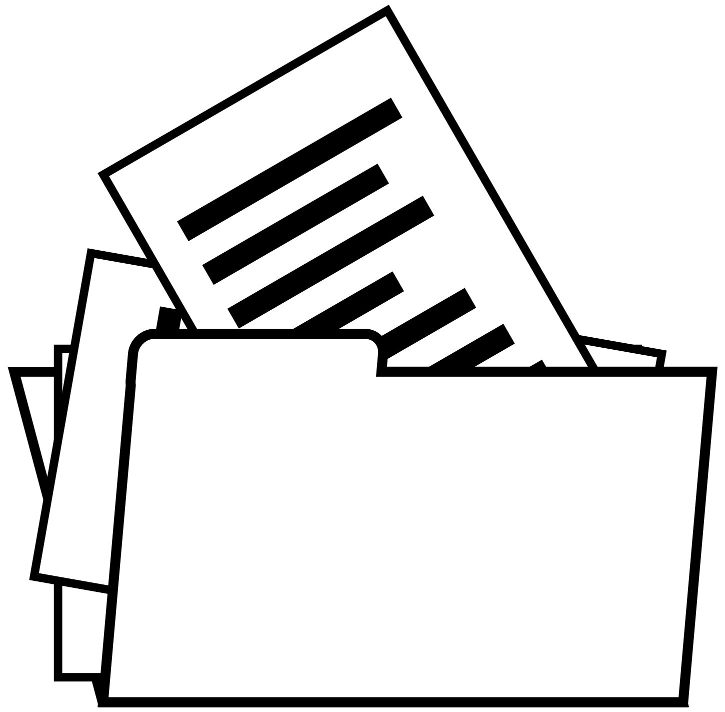


LITERATURE SURVEY OVERVIEW

06: Attention-CNN-LSTM IDS for In-Vehicle Networks

This study develops an IDS optimized for automotive environments by integrating convolutional networks, recurrent sequence modeling, and attention mechanisms.

Limitation: The model demands considerable computational power and large labeled datasets, which may limit deployment on embedded systems..

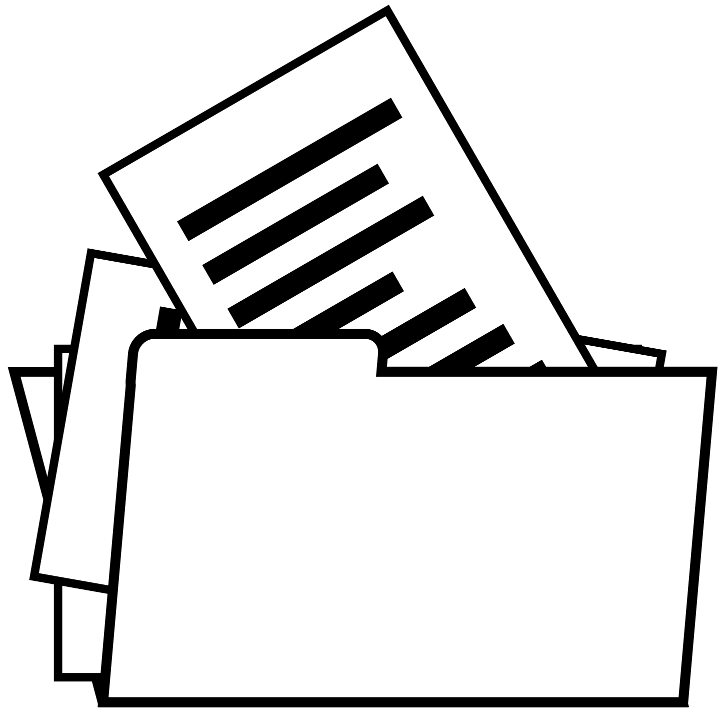


LITERATURE SURVEY OVERVIEW

07: Cognitive-Based IDS Using DNN + SVM

This research proposes a hybrid IDS that combines deep learning-based feature extraction with SVM-based classification to enhance the precision of anomaly detection.

Limitation: Its performance on modern datasets remains uncertain due to the aging nature of KDD99. The dual-model pipeline may also increase computation overhead.



PROPOSED SOLUTION

HYBRID FRAMEWORK (RL + GAN)

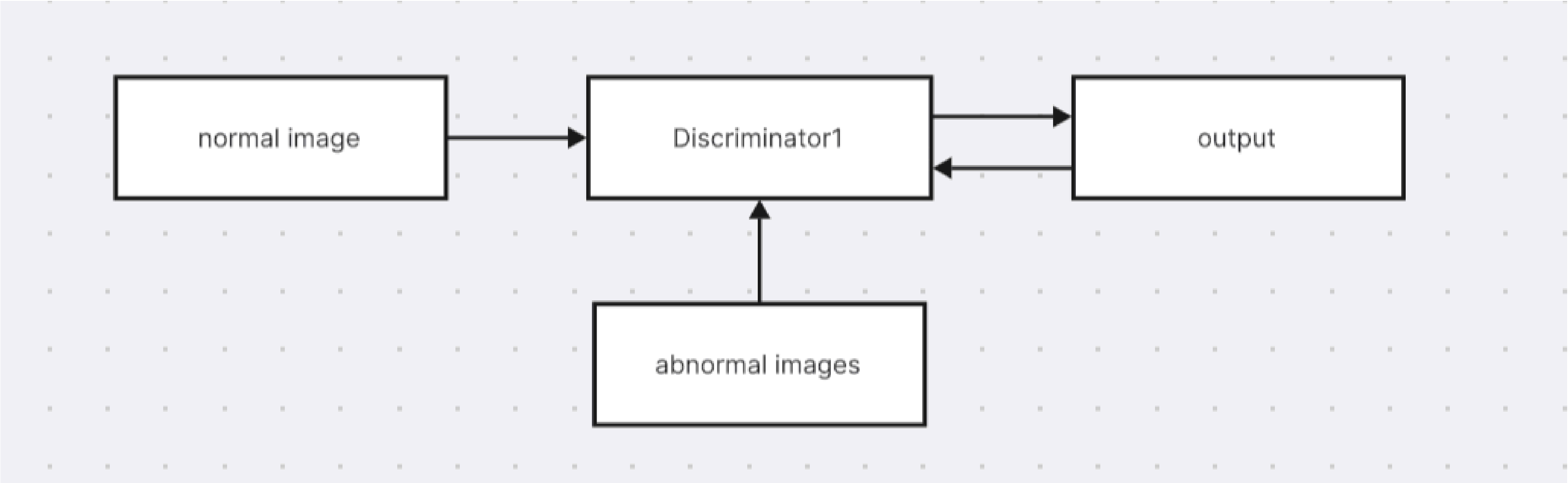
We propose a hybrid anomaly detection system that integrates Reinforcement Learning (RL) with a Generative Adversarial Network (GAN).

DATA PREPPROCESSING

One-hot encoding applied to create a 2D matrix. Converts identifiers into compact image-like representations for CNN processing.

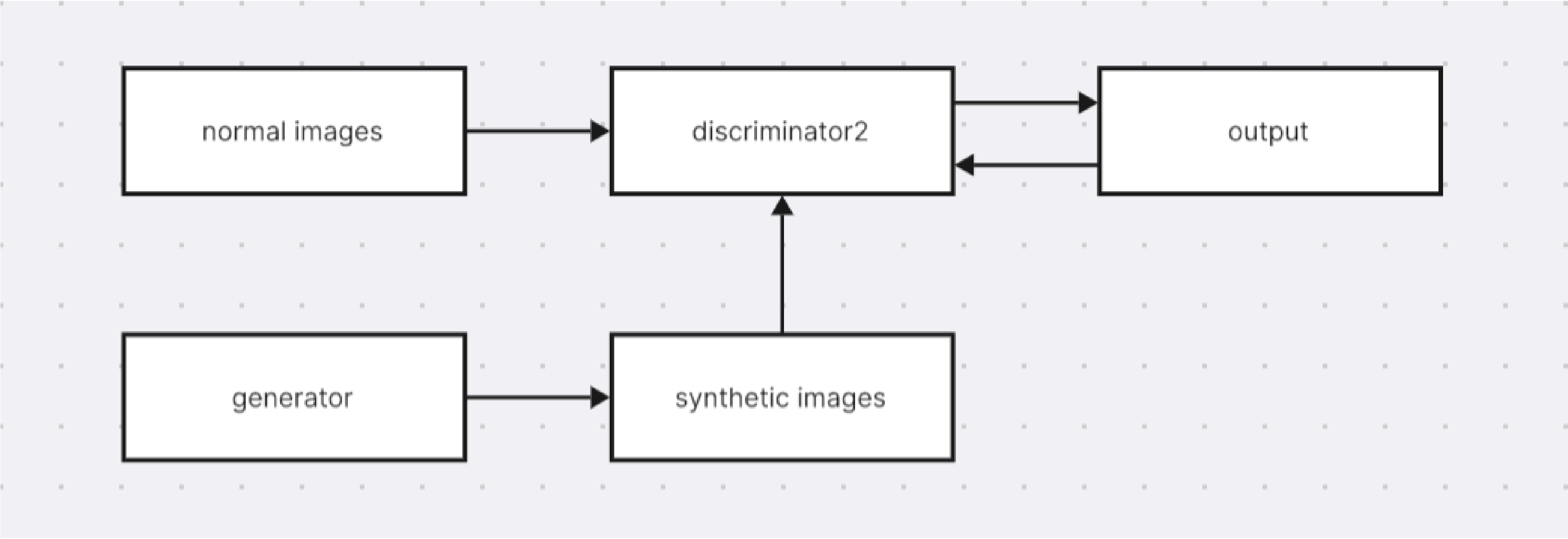
PROPOSED SOLUTION

MODEL ARCHITECTURE



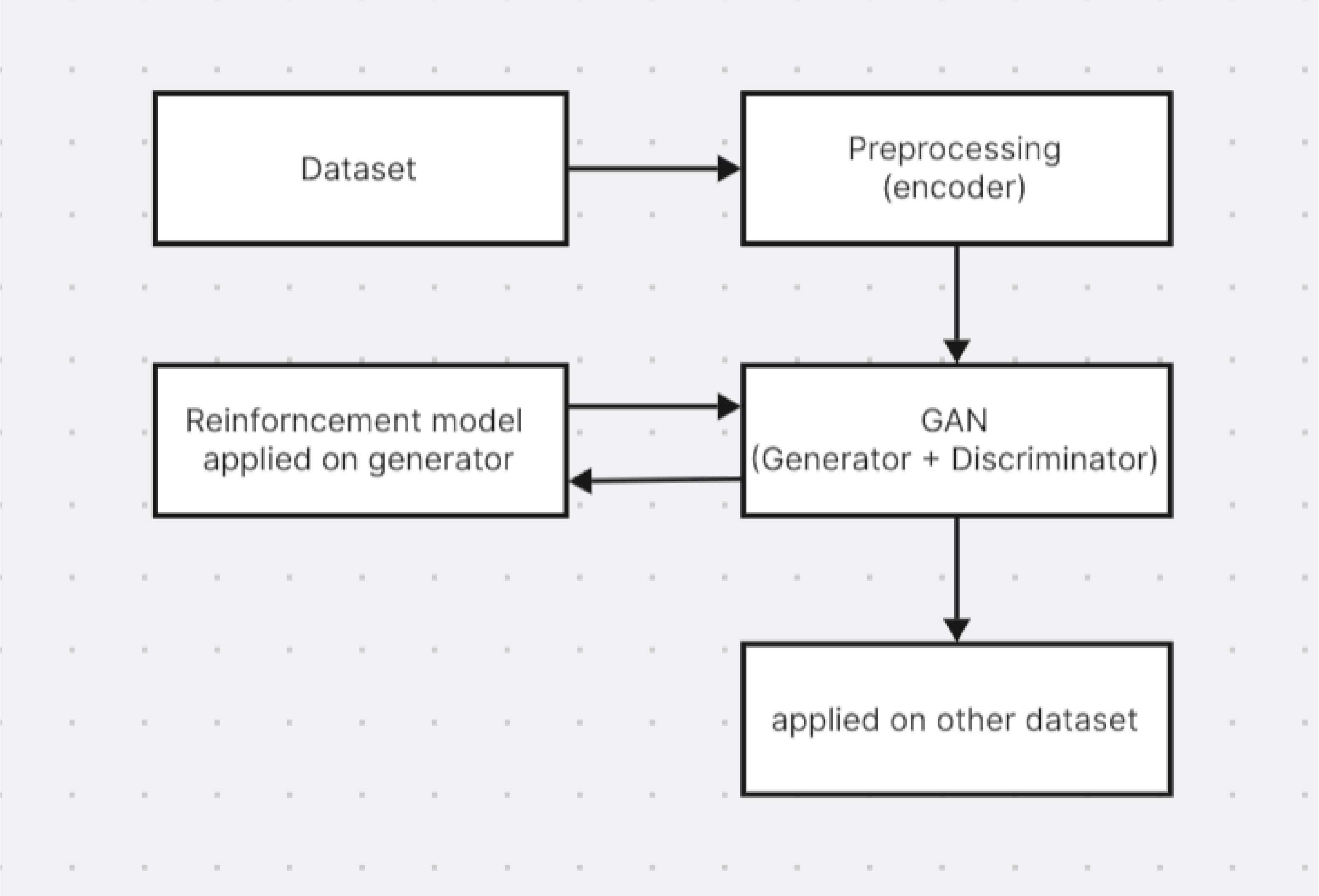
Discriminator 1

Discriminator 2



PROPOSED SOLUTION

MODEL ARCHITECTURE



Dataset

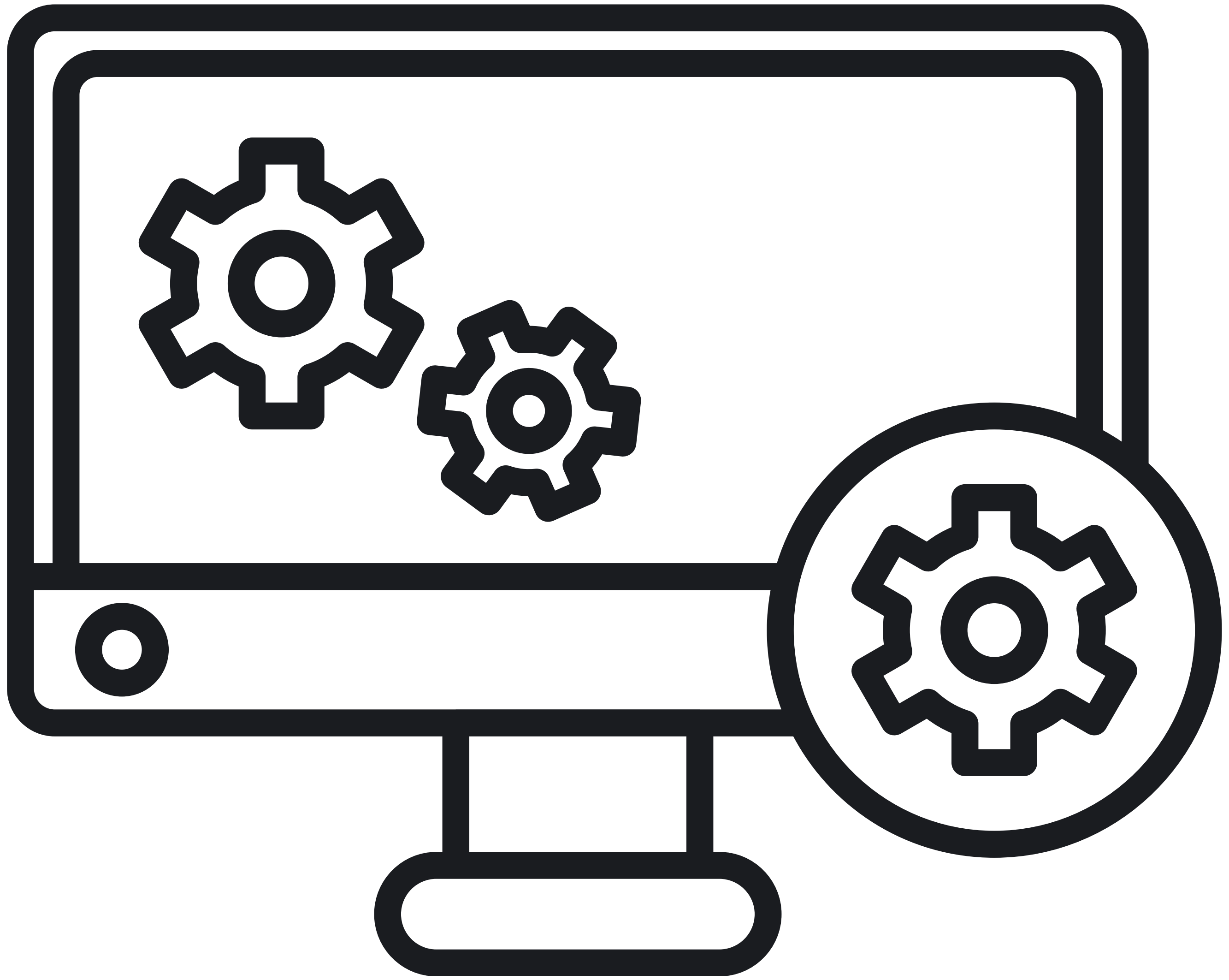
Preprocessing (encoder)

Reinforncement model applied on generator

GAN (Generator + Discriminator)

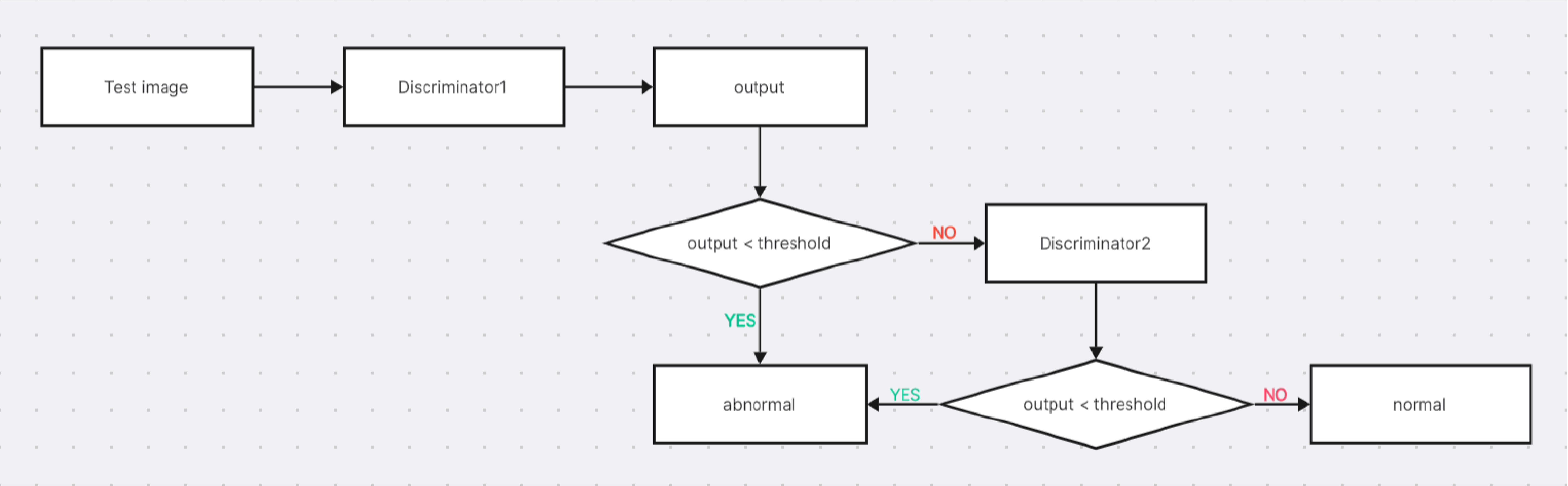
applied on other dataset

RL + GAN

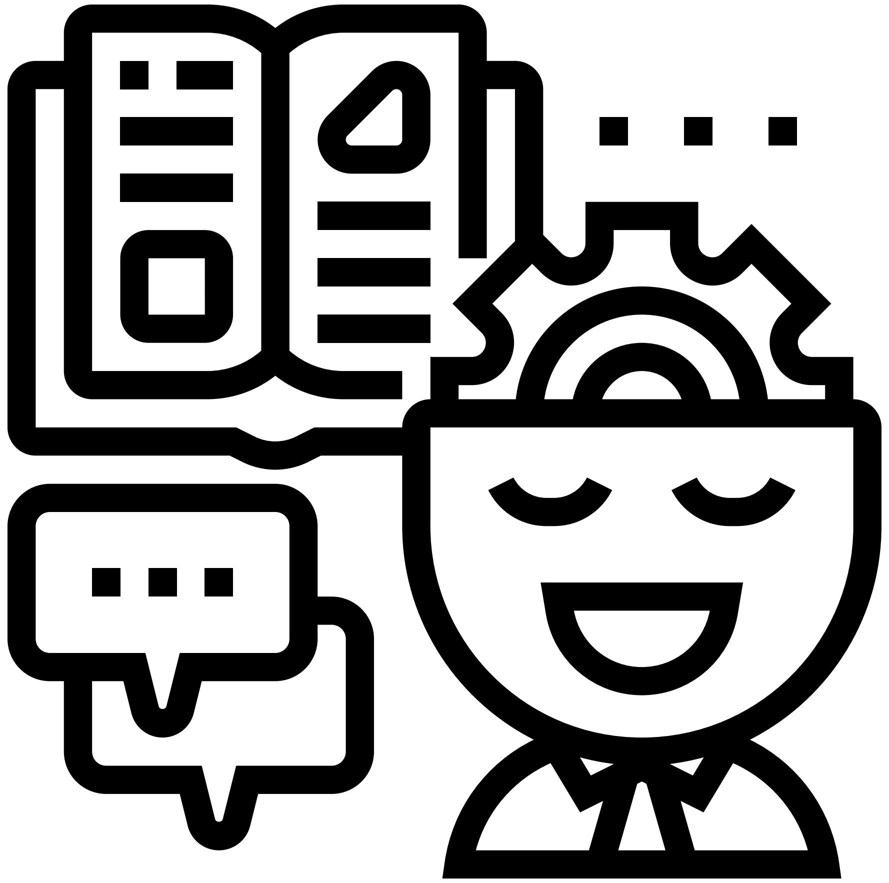


PROPOSED SOLUTION

MODEL ARCHITECTURE



Testing



CONCLUSIONS

Modern vehicles rely extensively on advanced electronics and connectivity, increasing their vulnerability to cybersecurity threats, particularly within the CAN bus protocol. Traditional intrusion detection techniques often lack the accuracy and adaptability needed to counter evolving attacks, emphasizing the necessity for intelligent, data-driven detection approaches capable of analyzing complex CAN traffic. By leveraging real vehicular datasets, understanding attack behaviors, and evaluating detection strategies, this research strengthens the security, reliability, and resilience of vehicle systems. Enhancing cybersecurity builds trust in connected and autonomous transportation and requires strong collaboration between researchers, manufacturers, and cybersecurity professionals.

REFERENCES

- K. Ren, Z. Li, X. Wang and Y. Zhang, "MAFSIDS: A reinforcement learning-based intrusion detection model for multi-intelligence feature selection networks," Journal of Big Data, vol. 10, Article 98, 2023

- K. Ren, J. Shen, X. Zhao, et al., "ID-RDRL: A deep reinforcement learning-based feature selection intrusion detection model," Scientific Reports, vol. 12, Article number (2022)

- C. Strickland, C. Saha, M. Zakar, S. Nejad, N. Tasnim, D. Lizotte and A. Haque, "DRL-GAN: A Hybrid Approach for Binary and Multiclass Network Intrusion Detection," Sensors (Basel), vol. 24, no. 9, Art. 2746, Apr. 2024. doi:10.3390/s24092746.

- M. Mouyart, G. Medeiros Machado and J.-Y. Jun, "A Multi-Agent Intrusion Detection System Optimized by a Deep Reinforcement Learning Approach with a Dataset Enlarged Using a Generative Model to Reduce the Bias Effect," Journal of Sensor and Actuator Networks, vol. 12, no. 5, 2023. DOI: 10.3390/jsan12050068.

- Z. Dai, Y. Yang, H. Zhang, et al., "An intrusion detection model to detect zero-day attacks in unseen data using machine learning," (open access), 2024 — autoencoder + supervised hybrid methodology evaluated on CIC-MalMem-2022. A

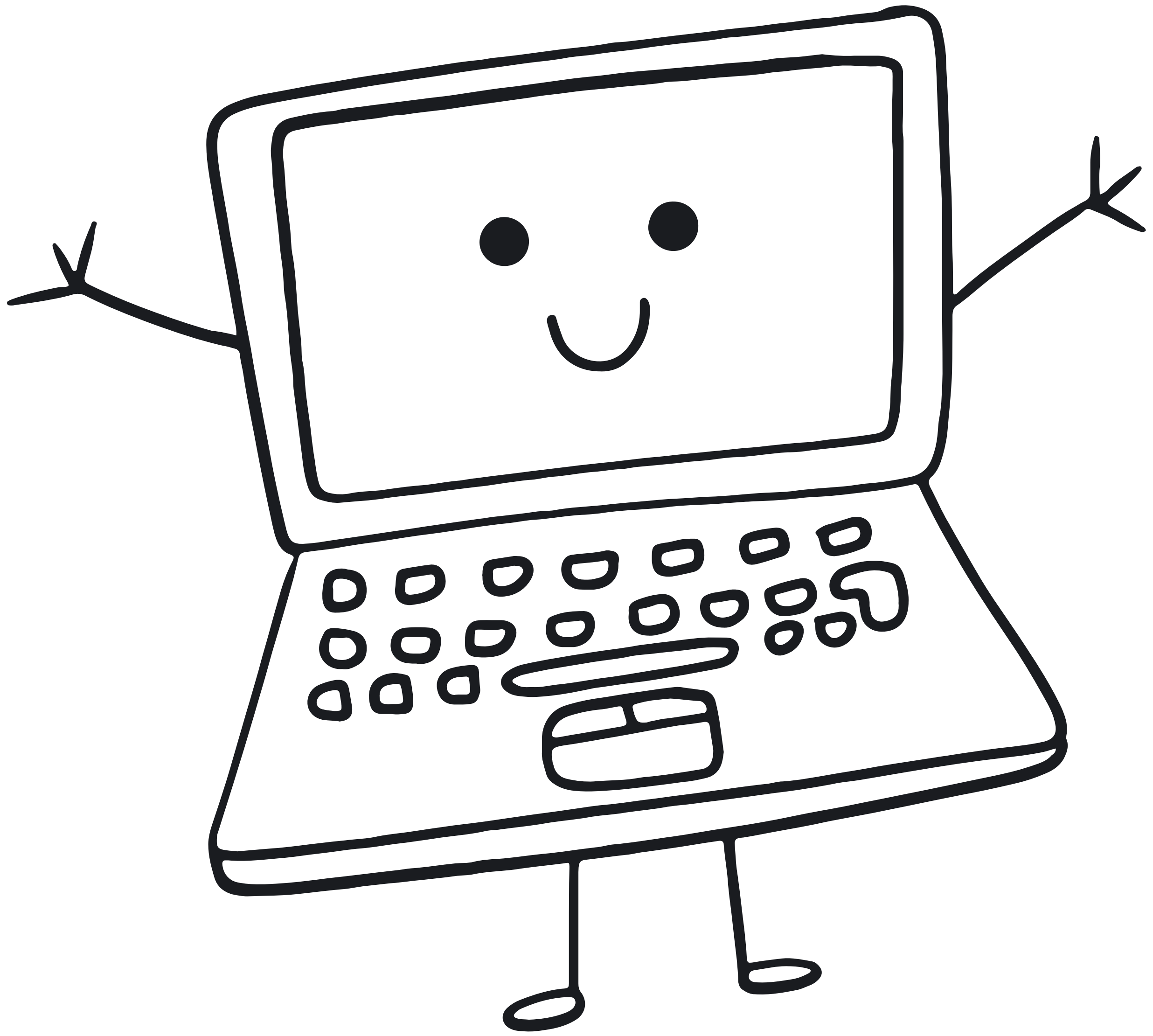
REFERENCES

- W. Yang, A. Acuto, Y. Zhou and D. Wojtczak, “A Survey for Deep Reinforcement Learning Based Network Intrusion Detection,” arXiv:2410.07612, Sep. 2024.

- A. M. Alashjaee, et al., “Attention-CNN-LSTM based intrusion detection (ACL-IDS): hybrid deep model for network/vehicle traffic,” Scientific Reports / relatedvenue, 2025. (See published work describing CNN+LSTM+attention for network/vehicle traffic; referenced in surveys).

- S. Parhizkari, “A cognitive-based method for intrusion detection systems: Deep neural features with SVM classification,” arXiv:2005.09436, 2020.

- S. M. Kasongo, “Performance Analysis of Intrusion Detection Systems Using Machine Learning Techniques and Feature Selection on UNSW-NB15,” Doctoral thesis / technical report, 2020.



THANK YOU