INTRUSION DETECTION SYSTEM IN CAN PROTOCOL

Solution proposed by
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.

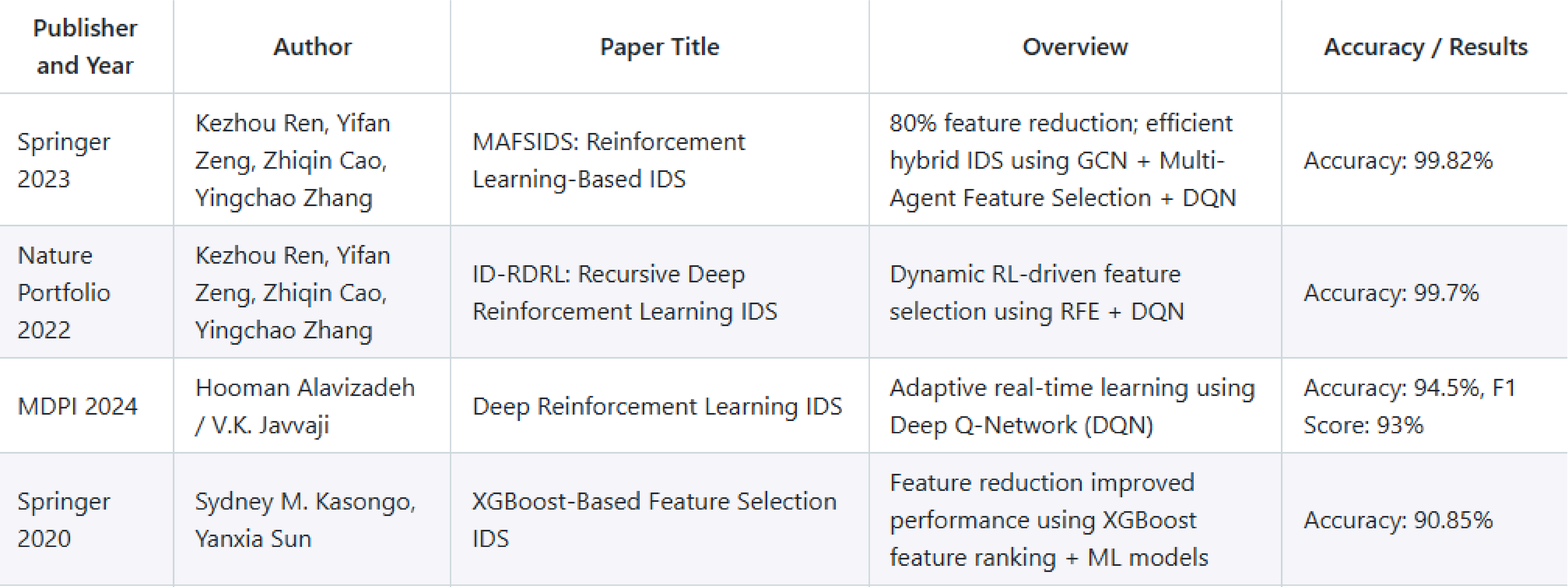
OBJECTIVE

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.

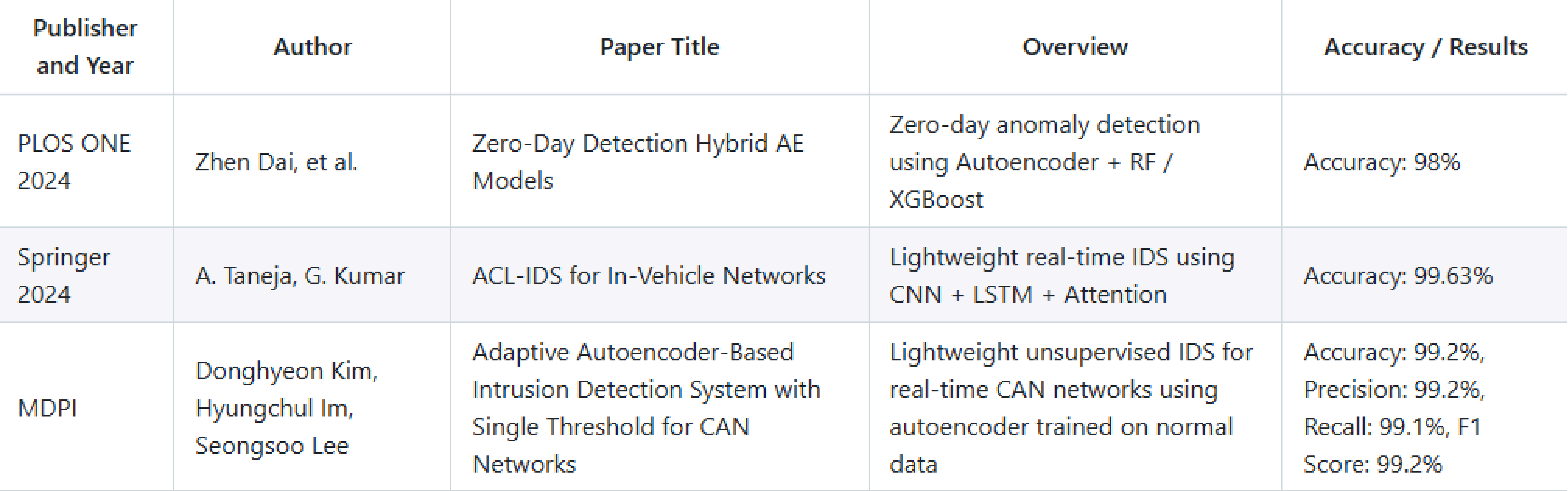
Data-Driven Detection
Utilize Machine Learning to model real-world patterns rather than relying on handcrafted rules.

LITERATURE SURVEY



Publisher and Year	Author	Paper Title	Overview	Accuracy / Results
Springer 2023	Kezhou Ren, Yifan Zeng, Zhiqin Cao, Yingchao Zhang	MAFSIDS: Reinforcement Learning-Based IDS	80% feature reduction; efficient hybrid IDS using GCN + Multi-Agent Feature Selection + DQN	Accuracy: 99.82%
Nature Portfolio 2022	Kezhou Ren, Yifan Zeng, Zhiqin Cao, Yingchao Zhang	ID-RDRL: Recursive Deep Reinforcement Learning IDS	Dynamic RL-driven feature selection using RFE + DQN	Accuracy: 99.7%
MDPI 2024	Hooman Alavizadeh / V.K. Javvaji	Deep Reinforcement Learning IDS	Adaptive real-time learning using Deep Q-Network (DQN)	Accuracy: 94.5%, F1 Score: 93%
Springer 2020	Sydney M. Kasongo, Yanxia Sun	XGBoost-Based Feature Selection IDS	Feature reduction improved performance using XGBoost feature ranking + ML models	Accuracy: 90.85%

LITERATURE SURVEY



Publisher and Year	Author	Paper Title	Overview	Accuracy / Results
PLOS ONE 2024	Zhen Dai, et al.	Zero-Day Detection Hybrid AE Models	Zero-day anomaly detection using Autoencoder + RF / XGBoost	Accuracy: 98%
Springer 2024	A. Taneja, G. Kumar	ACL-IDS for In-Vehicle Networks	Lightweight real-time IDS using CNN + LSTM + Attention	Accuracy: 99.63%
MDPI	Donghyeon Kim, Hyungchul Im, Seongsoo Lee	Adaptive Autoencoder-Based Intrusion Detection System with Single Threshold for CAN Networks	Lightweight unsupervised IDS for real-time CAN networks using autoencoder trained on normal data	Accuracy: 99.2%, Precision: 99.2%, Recall: 99.1%, F1 Score: 99.2%

BASE PAPER

Adaptive Autoencoder Based IntrusionDetection System with Single Threshold for CAN Networks
published by MDPI in July 2025

BASE PAPER APPROACH

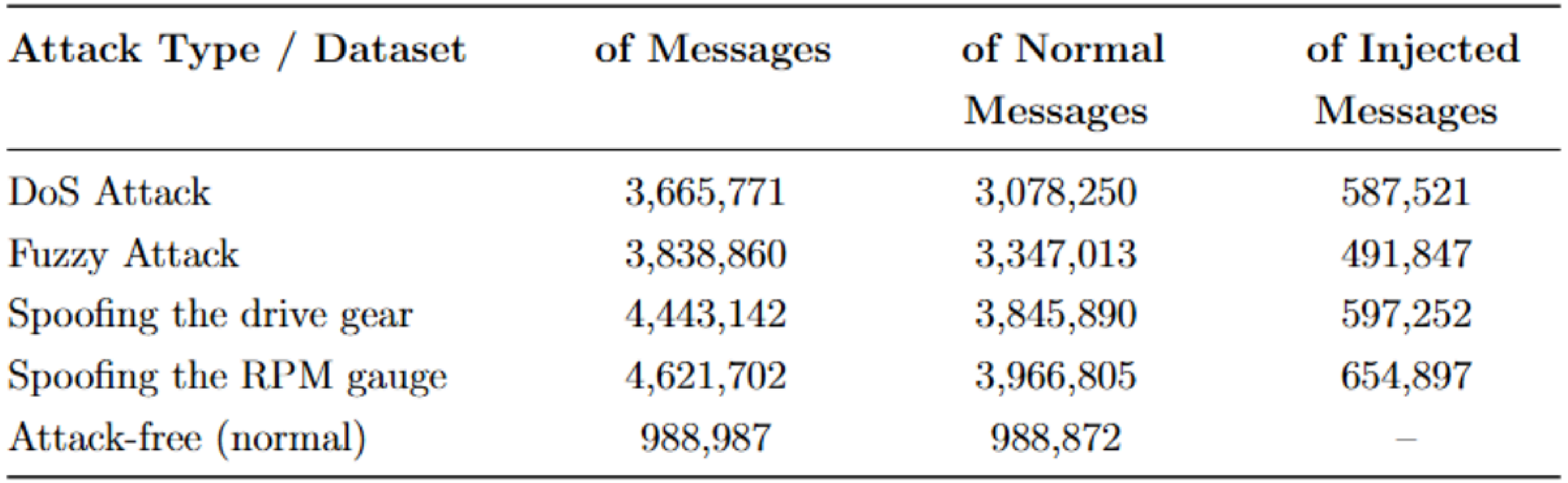
- Autoencoder trained only on normal CAN traffic
- Input: Sliding window of CAN frames
- Output: Reconstruction error (MSE)
- Single threshold used for attack detection
- The system detects attacks when reconstruction error exceeds a predefined threshold

KEY LIMITATION

- Designed primarily for binary detection (Normal vs Attack)
- Limited capability to classify specific attack types
- Detection performance depends heavily on threshold selection
- May struggle with subtle or low-intensity unseen attacks

PROPOSED SOLUTION

DATASET



Attack Type / Dataset	of Messages	of Normal Messages	of Injected Messages
DoS Attack	3,665,771	3,078,250	587,521
Fuzzy Attack	3,838,860	3,347,013	491,847
Spoofing the drive gear	4,443,142	3,845,890	597,252
Spoofing the RPM gauge	4,621,702	3,966,805	654,897
Attack-free (normal)	988,987	988,872	–

DATA ATTRIBUTES

Timestamp, CAN ID, DLC, DATA[0], DATA[1], DATA[2], DATA[3], DATA[4], DATA[5], DATA[6], DATA[7], Flag

- Timestamp : recorded time (s)
- CAN ID : identifier of CAN message in HEX
- DLC : number of data bytes, from 0 to 8
- DATA[0-7] : data value
- Flag : T or R, T represents injected message while R represents normal message

PROPOSED SOLUTION

HYBRID FRAMEWORK

We propose a hybrid intrusion detection system that integrates:

- Supervised LSTM-based multi-class classification
- Unsupervised Autoencoder-based anomaly detection

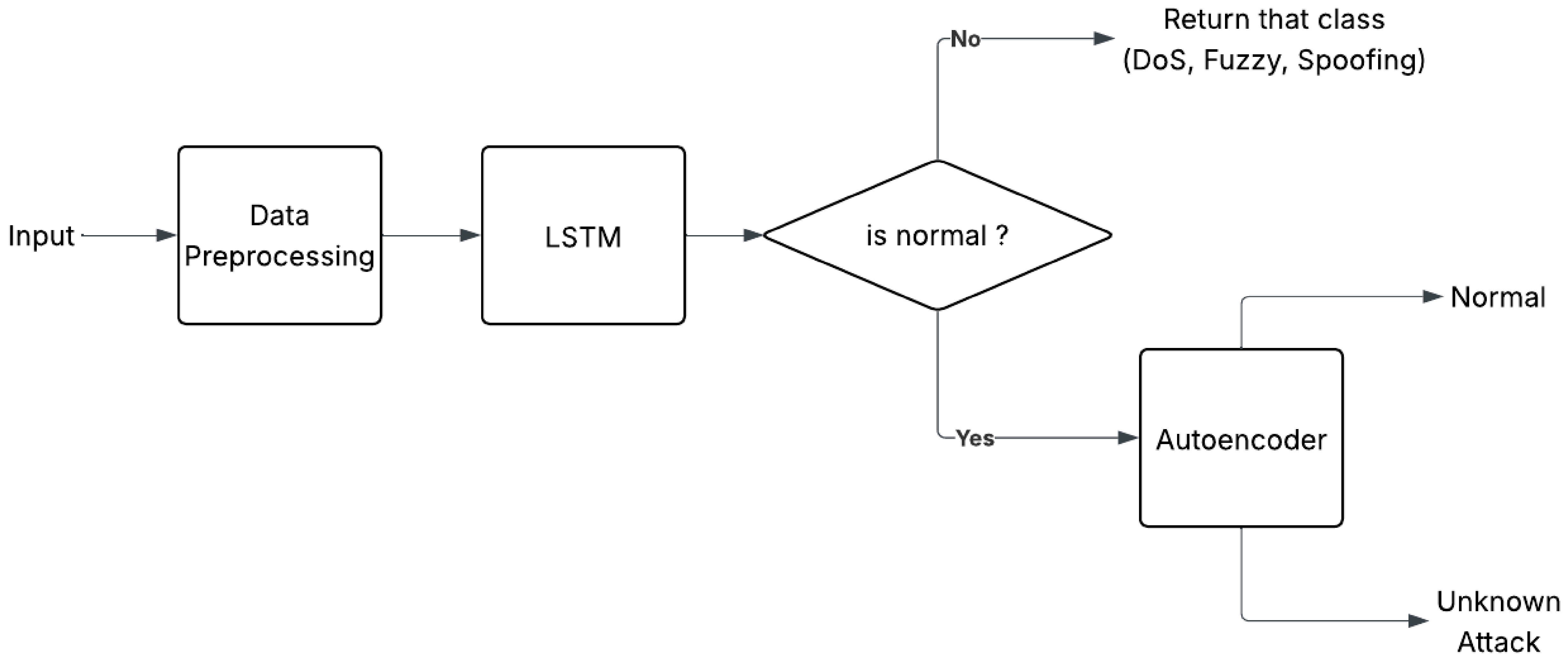
The LSTM detects known attack categories using temporal sequence modeling.

The Autoencoder models normal CAN behavior and identifies unseen or zero-day attacks using reconstruction error.

This two-stage architecture improves detection accuracy and generalization capability

PROPOSED SOLUTION

MODEL ARCHITECTURE



FUTURE SCOPE

- Test the system on more types of attacks
- Extend the system to support newer vehicle communication protocols
- Integrate the system into a real in-vehicle monitoring setup
- Optimising the system by using variational Autoencoder ot LSTM with attention mechanism

CONCLUSIONS

Modern vehicles require intelligent intrusion detection systems due to vulnerabilities in CAN communication.

The proposed Hybrid LSTM + Autoencoder framework:

- Detects known attacks using temporal sequence modeling
- Identifies unseen attacks through anomaly detection
- Uses KDE-based threshold for robust separation
- Maintains scalability for real-time automotive deployment

REFERENCES

[1] K. Ren, Y. Zeng, Z. Cao and Y. Zhang, “MAFSIDS: A reinforcement learning-based intrusion detection model for multi-agent feature selection networks,” Journal of Big Data, vol. 10, Article 98, 2023. Published by Springer.

[2] K. Ren, Y. Zeng, Z. Cao and Y. Zhang, “ID-RDRL: A deep reinforcement learning-based feature selection intrusion detection model,” Scientific Reports, vol. 12, 2022. Published by Nature Portfolio.

[3] H. Alavizadeh and V. K. Javvaji, “Deep reinforcement learning-based intrusion detection system for adaptive network security,” Electronics, vol. 13, 2024. Published by MDPI

[4] S. M. Kasongo and Y. Sun, “Performance analysis of intrusion detection systems using machine learning techniques and feature selection on UNSW-NB15,” Journal of Big Data, vol. 7, Article 99, 2020. Published by Springer.

REFERENCES

[5] Z. Dai, Y. Yang, H. Zhang, et al., “An intrusion detection model to detect zero-day attacks in unseen data using machine learning,” PLOS ONE, vol. 19, 2024. Published by Public Library of Science.

[6] A. Taneja and G. Kumar, “Attention-CNN-LSTM based intrusion detection system (ACL-IDS) for in-vehicle networks,” Soft Computing, 2024. Published by Springer.

[7] D. Kim, H. Im and S. Lee, “Adaptive autoencoder-based intrusion detection system with single threshold for CAN networks,” Sensors, vol. 25, no. 13, Article 4174, 2025. Published by MDPI.

[8] Dataset: Car Hacking Dataset

THANK YOU