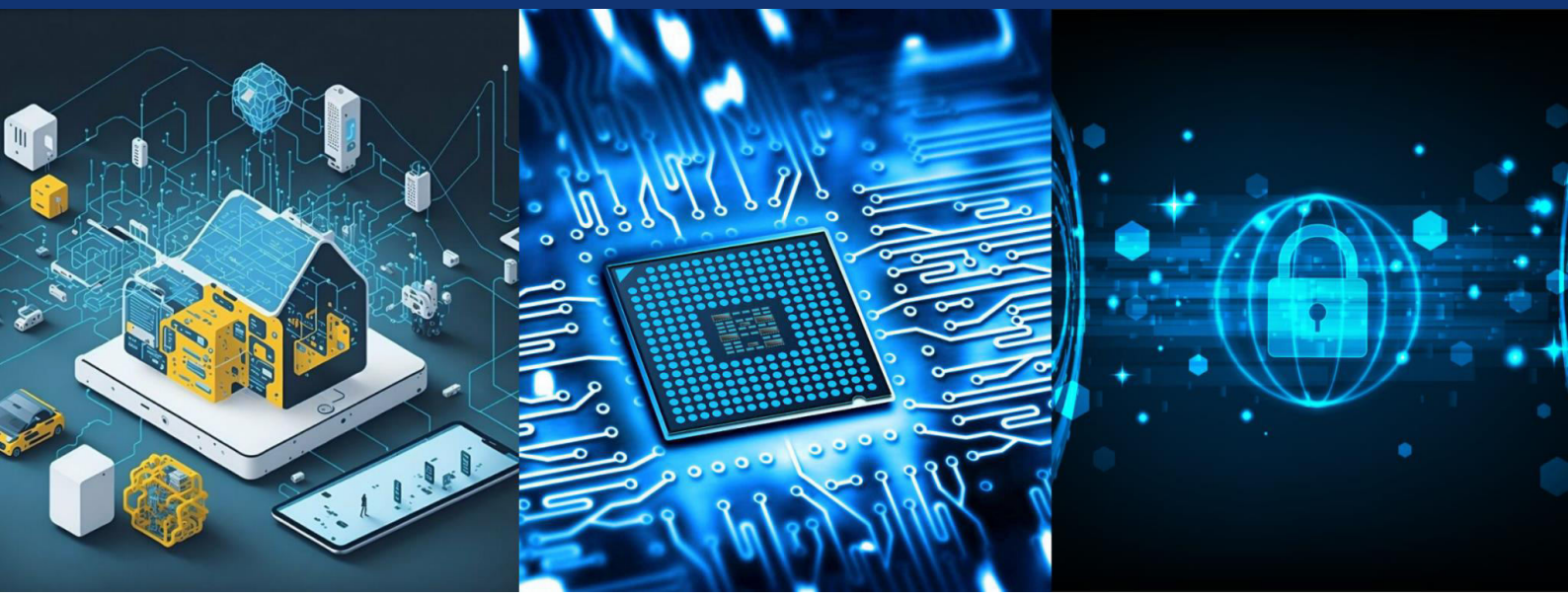
IJIRCCE

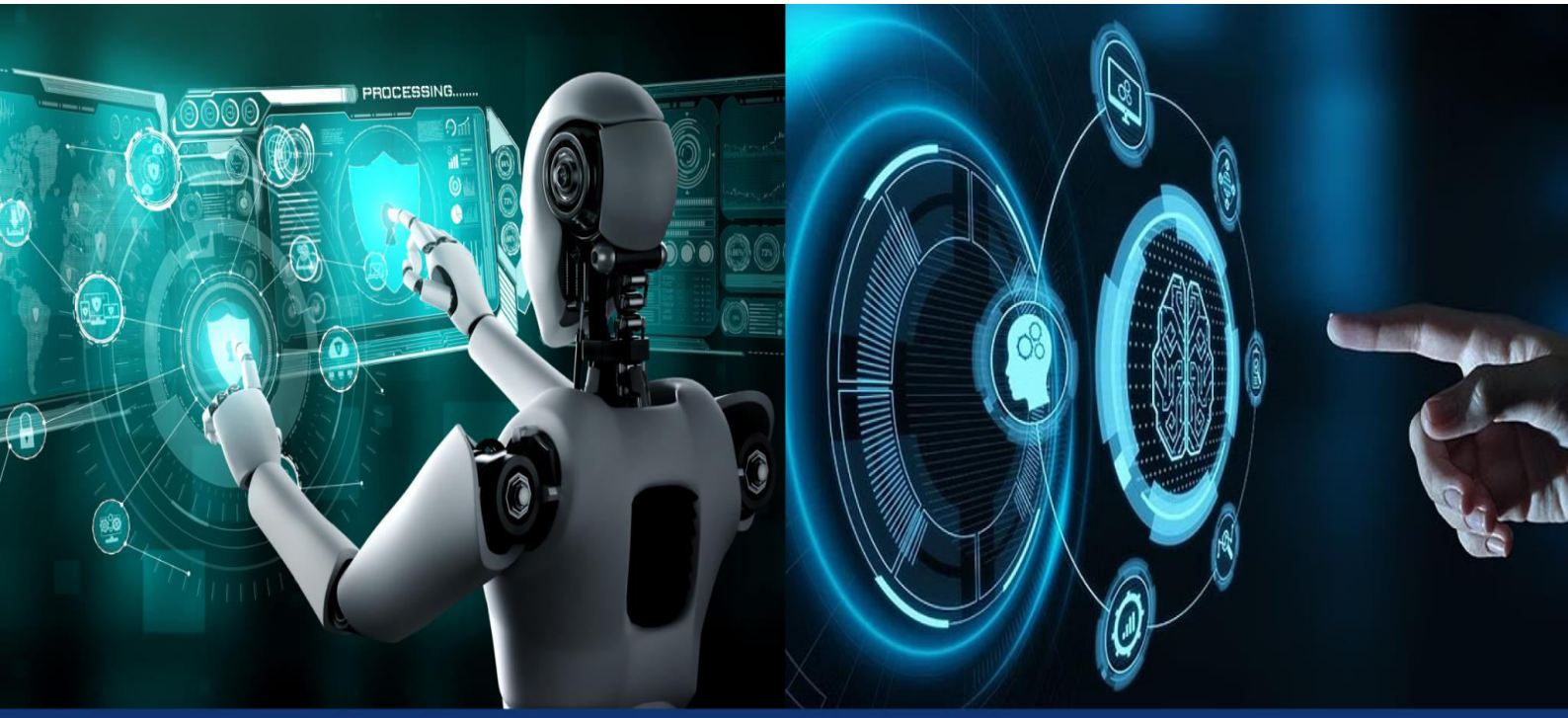
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 5, May 2025

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305161

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Detecting Unknown Cyber Attacks for Intra Vehicles using Recurrence Plots and Neural Network

C. Soundarya

Assistant Professor, Dept. of CSE, The Kavery Engineering Collage, Salem, Tamil Nadu, India

K. Sathesh, K. Poovarasan, R. Vignesh, C. Santhosh

UG Student, Dept. of CSE, The Kavery Engineering Collage, Salem, Tamil Nadu, India

Abstract: In-vehicle communication has become an integral part of today's driving environment considering the growing add-ons of sensor-centric communication and computing devices inside a vehicle for a range of purposes including vehicle monitoring, physical wiring reduction, and driving efficiency. However, related on cyber security for Intra-Vehicle Communication systems is still lacking potential dedicated solutions for in vehicle cyber risks. Existing solutions are mainly relying on protocol-specific security techniques and lacking an overall security framework for in-vehicle communication. However, it lacks security features. Conventional security mechanisms fail to protect in vehicle networks from attacks, requiring the development of an effective Intrusion Detection System (IDS). Machine Learning (ML)-based IDS for detecting novel cyber attacks in intra-vehicle networks, specifically in Controller Area Networks (CANs). This work develops an IDS for intra-vehicle networks called IDS-IVN based on a compact representation of location invariant and time-variant traffic features using deep learning..

I. INTRODUCTION

The ubiquitous nature of emerging V2X connectivity systems offers novel services and applications that enable advanced functions and features for modern vehicles, such as Advanced Driver Assistance Systems (ADAS), infotainment, productivity and maintenance services.For a safe, efficient, and comfortable operation of modern vehicles, data is transmitted through intra-vehicle and over inter-vehicle networks depending on system-level requirements. This provides new cyber-attack surfaces for potential intrusions into the vehicle systems, which can put road users' lives at risk if exploited by malicious agents.Modern vehicles are complex cyber-physical systems that embed different components, including Electrical Control Units (ECUs), sensors and actuators. The Controller Area Network (CAN) forms the communication backbone of most vehicles over which these components exchange data. Unfortunately, the CAN protocol has inherent cybersecurity vulnerabilities due to the lack of authentication mechanisms and the broadcasting nature of its communication method.

Objective

Effective Detection of Unknown Attacks: Develop a novel detection framework that utilizes recurrence plots and neural networks to accurately identify previously unknown and emerging cyber-attacks within intra-vehicle networks.

• **Pattern Recognition and Anomaly Detection:** Leverage the power of recurrence plots to transform time-series data into visual representations, enabling neural networks to effectively detect anomalous patterns and deviations from normal communication behavior.

• **Low-Latency Detection:** Ensure that the proposed method can perform real-time attack detection with minimal latency, maintaining the safety and security of critical automotive systems without compromising performance.

II. RELATED WORK

2.1 Cyberattacks and Countermeasures for In-Vehicle Networks

Aliwa et al (2020) defined as, connectivity between and within vehicles increases, so does concern about safety and security. Various automotive serial protocols are used inside vehicles such as Controller Area Network (CAN), Local Interconnect Network (LIN) and FlexRay.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305161

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

CAN bus is the most used in-vehicle network protocol to support exchange of vehicle parameters between Electronic Control Units (ECUs). This protocol lacks security mechanisms by design and is therefore vulnerable to various attacks.

2.2 In-Vehicle Communication Cyber Security: Challenges and Solutions

Computer vision techniques have been increasingly applied to facial palsy assessment. Early work by Neely et al. [7] used video analysis to measure facial movement. Wang et al. [8] developed a system using facial landmark detection to quantify facial asymmetry.

Recent approaches have leveraged deep learning techniques. Kim et al. [9] used convolutional neural networks (CNNs) to classify facial palsy severity from images. Fujiwara et al. [10] developed a model combining facial landmark detection with CNN classification, achieving 94.5% accuracy in identifying facial palsy.

2.3 Web-Based Medical Diagnostic Tools

Rathore, R.S et al (2022) defined as, In-vehicle communication has become an integral part of today's driving environment considering the growing add-ons of sensor-centric communication and computing devices inside a vehicle for a range of purposes including vehicle monitoring, physical wiring reduction, and driving efficiency. However, related literature on cyber security for in-vehicle communication systems is still lacking potential dedicated solutions for in-vehicle cyber risks

2.4 Using DeepLearning Networks to Identify Cyber Attacks on Intrusion Detection for In-Vehicle Networks

Lin, H.-C et al (2022) described to enable various intelligent functions, the electrical system of existing vehicles incorporates a controller area network (CAN) bus system that enables communication among electrical control units (ECUs). In practice, traditional network-based intrusion detection systems (NIDSs) cannot easily identify threats to the CAN bus system. Therefore, it is necessary to develop a new type of NIDS—namely, on-the-move Intrusion Detection System (OMIDS)—to categorise these threats.

III. SYSTEM ARCHITECTURE AND METHODOLOGY

3.1 System Overview

This section introduces the non-technical terminology used in the narrative form of the system. It should provide a high-level system architecture diagram representing the subsystem subfields of the system, if applicable. High-level system architecture or subsystem diagrams should, if applicable, show interfaces to external systems. Provides high-level contextual diagrams of systems and subsystems, if applicable. To identify the functional requirements assigned to this design document, refer to the Requirements Traceability Matrix (RTM) in the Functional Requirements Document (FRD).

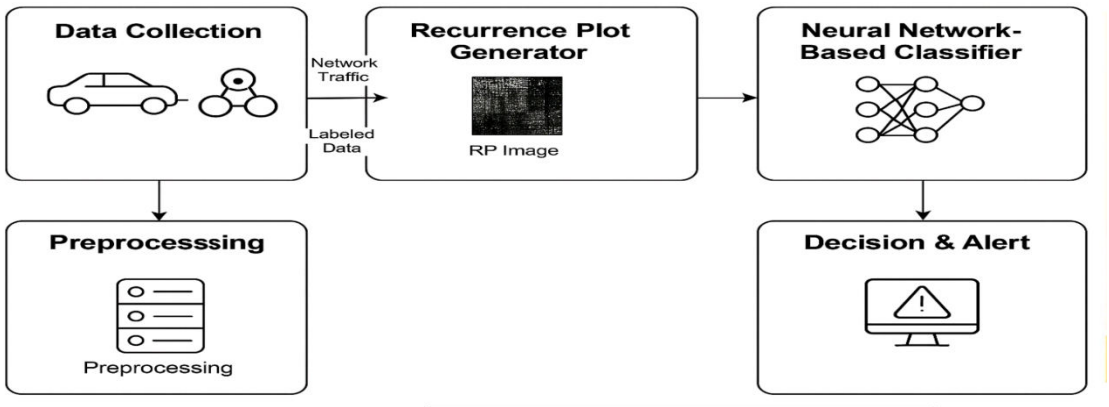


Figure 1: High-level architecture of the Detecting unknown cyber attack in intra vehicle network using recurrence plot and neural network

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305161

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

3.2 Web Applications

The web interface is designed to be intuitive and accessible across different devices. It allows users toWe can use Python to develop web applications. It provides a library that handles network protocols such as HTML, XML, JSON, email processing, requests, delicious soups, and parser feeds. It also provides frameworks such as Django, Pyramid, and Flask for designing and developing web-based application.

3.3 Desktop GUI Applications

Python provides Tk's GUI library for developing user interfaces for Python-based applications. Some other useful toolkits for width x widgets, Kivy, PyQt are available on several platforms. Kivy is a popular multi-touch application for writing.

3.4 Methodology

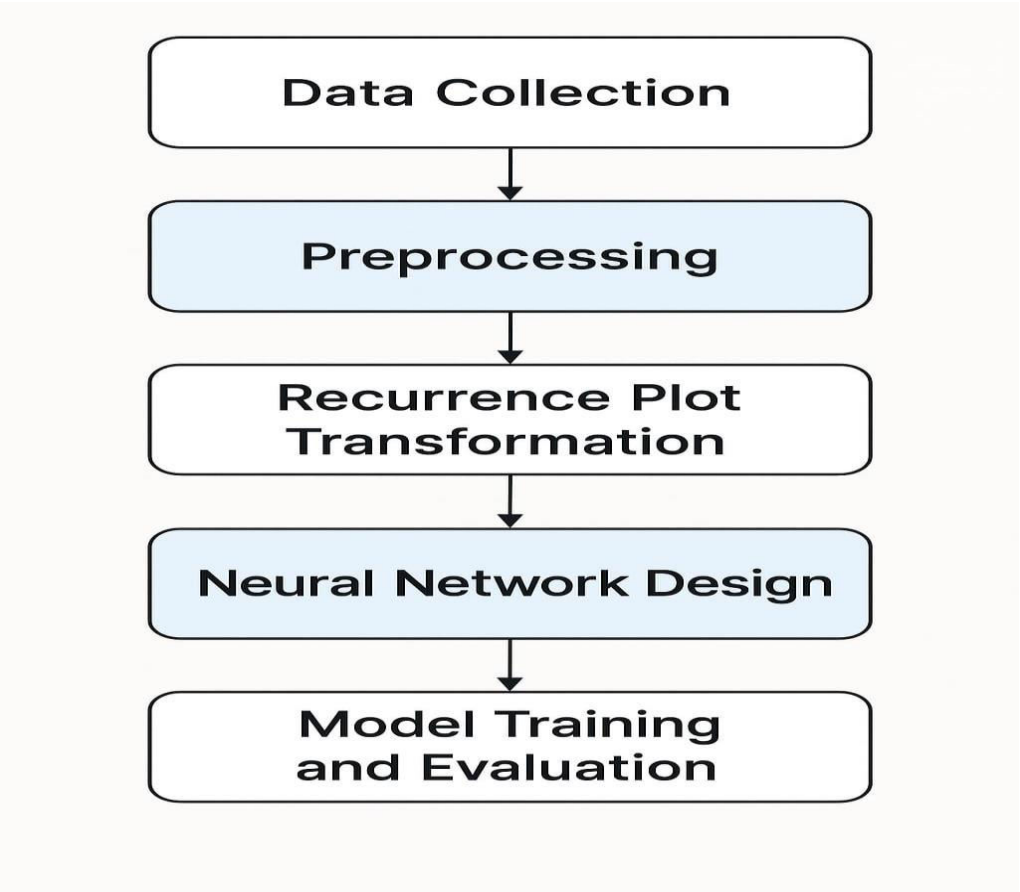


Figure 2: Methodology of Detection and deployment

3.4.1 Data Collection

Capture CAN bus traffic data from a real or simulated vehicle environment. Collect both benign and malicious data (including unknown attacks if possible). Tools: OBD-II scanners, CAN interfaces (e.g., CANtact, Vector), datasets like Car Hacking Dataset (from UNSW, Argus, etc.).

3.4.2 Preprocessing

Convert raw CAN frames into time-series data. Extract fields such as timestamp, CAN ID, data length, and data bytes. Apply normalization or scaling to standardize inputs.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305161

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

3.4.3 Recurrence Plot Transformation

A Recurrence Plot (RP) visualizes how a system's state at one time is similar to its state at another time.

Convert the time-series CAN data into 2D recurrence plots using:

Phase space reconstruction

Distance matrix computation

Binary thresholding to create the RP image

This process transforms temporal CAN data into an image format suitable for CNNs

3.4.3 Neural Network Design

Design a Convolutional Neural Network (CNN) or hybrid model (CNN + LSTM) to classify RP images.

Train the model using:

Labeled RP images (normal vs. attack) Use techniques like dropout, batch normalization, etc., to avoid overfitting.

3.4.4Model Training and Evaluation

Split the dataset into training, validation, and testing sets.

Use performance metrics like:

Accuracy

Precision, Recall,

F1-Score

Confusion matrix

ROC-AUC curve

Implement early stopping and hyperparameter tuning.

3.4.5 Detection and Deployment

Integrate the trained model with a real-time CAN bus monitoring system.

The model processes new CAN data, transforms it into RP, and classifies it as Normal or attack.

Unknown attacks can be identified due to the generalization power of deep learning on image-like inputs.

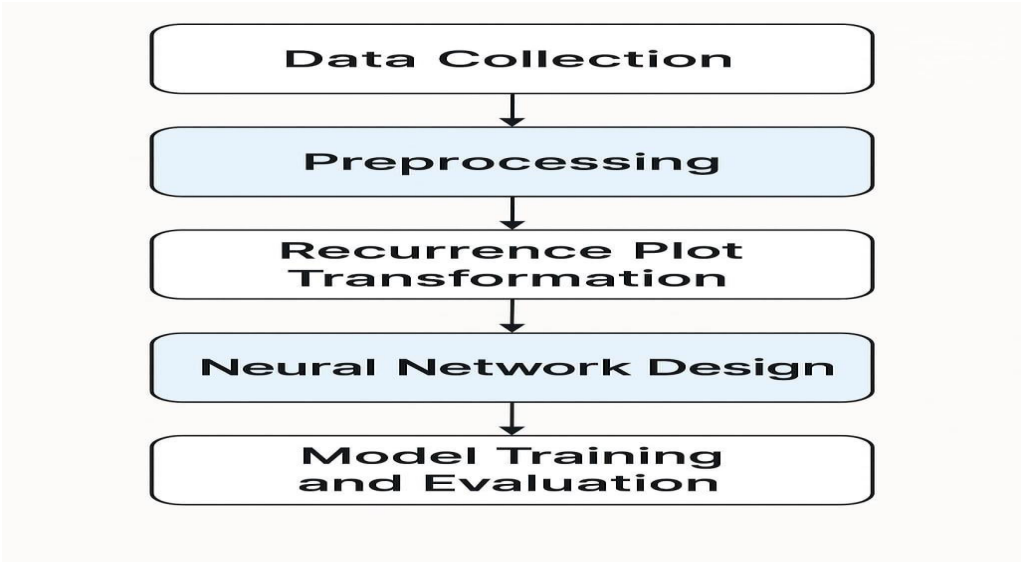


Figure 3: Classification model architecture

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305161

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. IMPLEMENTATION DETAILS

4.1 Development Environment

Hardware Requirements

- CPU type : Intel core i5 processor
- Ram size : 8 GB
- Hard disk capacity : 500 GB

Software Requirement

- Operating System : Windows 10
- Language : Python
- Tool Software Description : Anaconda

Following are important characteristics of Python Programming:

- It supports functional and structured programming methods as well as OOP.
- It can be used as a scripting language or can be compiled to byte-code for building large applications.
- It provides very high-level dynamic data types and supports dynamic type checking.
- It supports automatic garbage collection.
- It can be easily integrated with C, C++, COM, ActiveX, CORBA, and Java.

4.2 Data Set Architecture

Labels		Quantity
BENIGN		2,273,097
DoS Hulk		231,073
PortScan		158,930
DDoS		128,027
DoS GoldenEye		10,293
DoS Slowhttptest		5,499
FTP-Patator		7,938
SSH-Patator		5,897
DoS slowloris		5,796
Web Attack	Web Attack - Brute Force	2,180
	Web Attack - XSS	
	Web Attack - Sql Injection	
Bot		1,966
Infiltration		36
Heartbleed		11

Figure 4: Data set in module descriotion

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305161

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

4.3 Code Structure

Import packages

```
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
import seaborn as sns
import plotly.express as px

import numpy as np
from tensorflow.keras.models import Sequential
from tensorflow.keras.layers import SimpleRNN, Dense
from tensorflow.keras.optimizers import Adam
from sklearn.model_selection import train_test_split
from sklearn.metrics import accuracy_score
import warnings
warnings.filterwarnings("ignore")
```

Figure 5: import packages

V. EXPERIMENTAL RESULTS

	Timestamp	Source IP Address	Destination IP Address	Source Port	Destination Port	Protocol	Packet Length	Packet Type	Traffic Type	Payload Data	...	Action Taken	Severity Level	User Information	Infor
0	30-05-2023 06:33	103.216.15.12	84.9.164.252	31225	17616	ICMP	503	Data	HTTP	Qui natus odio asperiores nam. Optio nobis ius...	...	Logged	Low	Reyansh Dugal	Moz (compatibl 8.0; Windov
1	26-08-2024 07:08	78.199.217.198	66.191.137.154	17245	48166	ICMP	1174	Data	HTTP	Aperiam quos modi officiis veritatis rem. Omni...	...	Blocked	Low	Sumer Rana	Moz (compatibl 8.0; Windov
2	13-11-2022 08:23	63.79.210.48	198.219.82.17	16811	53600	UDP	306	Control	HTTP	Perferendis sapiente vitae soluta. Hic delectu...	...	Ignored	Low	Himmat Karpe	Moz (compatibl 9.0; Windov
3	02-07-2023 10:38	163.42.196.10	101.228.192.255	20018	32534	UDP	385	Data	HTTP	Totam maxime beatae expedita explicabo porro l...	...	Blocked	Medium	Fateh Kibe	Moz (Macinto Mac OS X 1

Figure5: Import Dataset:

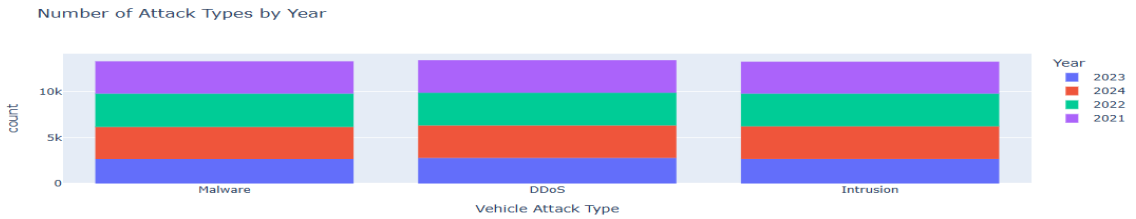


Figure 6: Attack types:

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305161

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Figure 7: Attack

Geo-location Data	Vehicle Attack Type	
Ghaziabad, Jharkhand	Intrusion	10
Aligarh, Chhattisgarh	Malware	9
Aurangabad, Nagaland	Malware	9
Srikakulam, Uttarakhand	Intrusion	8
Yamunanagar, Arunachal Pradesh	Malware	8
Rampur, Gujarat	Intrusion	8
Jalgaon, Mizoram	Malware	8
Amroha, Sikkim	Intrusion	8
Panvel, Jharkhand	Intrusion	8
Kochi, Tamil Nadu	DDoS	7
Ghaziabad, Meghalaya	Intrusion	7
Tenali, Madhya Pradesh	Malware	7
Ghaziabad, Nagaland	Malware	7
Pimpri-Chinchwad, Manipur	DDoS	7
Karnal, Tamil Nadu	Intrusion	7
Kottayam, Nagaland	Malware	7
Junagadh, Telangana	DDoS	7
Kadapa, Mizoram	Intrusion	7
Fatehpur, Gujarat	DDoS	7
Hospet, Gujarat	Malware	7

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. FUTURE WORK

Future research directions include:

1. Integration with Real-Time Vehicle Systems: Deploy the trained detection model into real in-vehicle ECUs to evaluate its performance under real-time driving conditions.
2. Extension to Other Automotive Protocols: Expand detection capabilities beyond CAN to include protocols like LIN, FlexRay, and Ethernet used in modern vehicles.
3. Improved Recurrence Plot Optimization: Explore adaptive and dynamic recurrence plot generation methods to improve the visualization of complex attack patterns.
4. Hybrid Deep Learning Models: Combine CNNs with other architectures like LSTM or Transformer networks to better capture temporal dependencies and improve classification accuracy.
5. Adversarial Attack Robustness: Evaluate the model's resistance to adversarial examples and develop defenses against adversarial manipulation.
6. Lightweight Model Deployment: Optimize and compress models for embedded systems to ensure low-latency detection with minimal resource usage.
7. Dataset Expansion and Benchmarking: Collect diverse and larger datasets with various attack scenarios and share them for benchmarking in the research community.

VII. CONCLUSION

Proposed an ML-based approach for intrusion detection in intra-vehicle networks. The proposed approach generates two representations/views of the CAN data leveraged by machine learning techniques.

The views provide high-level features capturing the time and intra-message dependencies of the CAN messages as well as their context. These views are concatenated and used to predict the class label of each message. The performance of the proposed approach was evaluated and compared with the state of-the-art detection techniques.

The results demonstrated that combining both views lead to better performance compared to a single view. The results also demonstrated that the proposed approach outperforms other state-of-the-art methods in detecting novel intrusions as it achieved the highest accuracy.

The possibility of improving the detection capability of the proposed approach could be investigated further. Despite that our method relies on the structure of CAN messages, we believe it could be easily extended for typical message addressing protocols.

REFERENCES

1. Aliwa, Emad & Rana, Omer & Perera, Charith & Burnap, Peter. (2020). Cyberattacks and Countermeasures 10.48550/arXiv.2004.10781.
2. Rathore, R.S.; Hewage, C.; Kaiwartya, O.; Lloret, J. In-Vehicle Communication Cyber Security: Challenges and Solutions. Sensors 2022, 22, 6679. https://doi.org/10.3390/s22176679.
3. Weiping Ding, Ibrahim Alrashdi, Hossam Hawash, Mohamed Abdel Basset,DeepSecDrive: An explainable deep learning framework for real-time detection of cyberattack in in-vehicle networks,Information Sciences,Volume 658,2024,120057,ISSN 0020-0255,https://doi.org/10.1016/j.ins.2023.120057.
4. Lin, Hsiao-Chung & Wang, Ping & Chao, Kuo-Ming & Lin, Wen-Hui & Chen, Jia-Hong. (2022). Using Deep Learning Networks to Identify Cyber Attacks on Intrusion Detection for In-Vehicle Networks. Electronics. 11. 2180. 10.3390/electronics11142180.
5. Haddaji A, Ayed S, Chaari Fourati L, Merghem Boulahia L. Investigation of Security Threat Datasets for Intra- and Inter-Vehicular Environments. Sensors (Basel). 2024 May 26;24(11):3431. doi: 10.3390/s24113431. PMID: 38894219; PMCID: PMC11174416.
6. Boualouache A., Engel T. A survey on machine learning-based misbehavior detection systems for 5g and beyond vehicular networks. IEEE Commun. Surv. Tutor. 2023;25:1128–1172. doi: 10.1109/COMST.2023.32364

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details