VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science Engineering and Information Systems

Department of Computer Applications

Winter Semester 2023-2024

SET CONFERENCE

First Review (28th February 2024)

Reg. No: 23MCA0028, 23MCA0056, 23MCA0076

Student Name: MOHAMED FAHEEJ N, MUDASSIR KHAN G, JASHWANTH KUMAR S

Guide Name: Prof Dr. Jayalakshmi.P

Paper Title: INTRUSION DETECTION SYSTEM FOR INTERNET OF VEHICLES USING OPTIMIZED CNN

Problem Description:

As the Internet of Things (IoT) paradigm continues to evolve, the integration of Internet of Vehicles (IoV) has become increasingly prevalent, enabling advanced connectivity and communication among vehicles and infrastructure. However, this interconnectedness also introduces significant security challenges, particularly regarding the detection and prevention of intrusions and cyber attacks within the vehicular network.The objective of this project is to develop an effective Intrusion Detection System (IDS) tailored specifically for Internet of Vehicles (IoV) environments. The IDS will be tasked with identifying and mitigating various types of intrusions, including malicious activities, anomalies, and cyber attacks, thereby ensuring the integrity, availability, and confidentiality of vehicular communication and data.

Literature Survey:

[1] The paper introduces a novel framework for cyber-attack detection in both intra-vehicle and external networks within the Internet of Vehicles (IoV) context. By leveraging convolutional neural networks (CNN), transfer learning, ensemble learning, and hyper-parameter optimization (HPO) techniques, the proposed Intrusion Detection System (IDS) aims to effectively identify various types of attacks targeting vehicle systems. The system collects and transforms intra-vehicle and external network data into images for analysis, enabling the detection of abnormal patterns indicative of cyber-attacks. Through experimentation on benchmark datasets like Car-Hacking and CICIDS2017, the IDS demonstrates high performance in terms of accuracy, precision, recall, and F1-scores. Additionally, the integration of ensemble learning enhances the robustness of the IDS by combining multiple models to improve detection capabilities. The framework's evaluation includes model training on a server-level machine and testing on a vehicle-level machine, showcasing its efficiency in real-world deployment scenarios. Overall, the proposed system offers a comprehensive approach to enhancing the security of connected vehicles by effectively detecting and mitigating cyber threats in both internal and external vehicular networks.

[2] The research paper focuses on implementing a Distributed Deep CNN-LSTM Model for Intrusion Detection in IoT-Based Vehicles. The system utilizes the Apache Spark framework to create a master-slave control structure for task scheduling, distribution, and fault tolerance. The master node manages these functions while the slave nodes perform parallel computing tasks. Data is stored using the HDFS storage system, and a combined deep learning algorithm is employed for intrusion detection. The system collects real-time Internet of Vehicles data, preprocesses and normalizes it, extracts features through convolution layers, and utilizes pooling layers for dimension reduction. By leveraging the Spark framework, the system offers high reliability, concurrency, and performance in handling diverse datasets. The use of deep learning algorithms, such as CNN-LSTM, enhances detection efficiency and reduces detection time, showcasing promising results in comparison to traditional methods. Overall, the system integrates distributed architecture, deep learning algorithms, and advanced technologies to improve security measures in IoT-based vehicles.

[3] The paper discusses the implementation of an Intrusion Detection System (IDS) in a vehicular network using a deep learning approach. The system utilizes safety-related messages exchanged through V2V communication to enhance security and reduce the risk of cyber-attacks in the automotive network. By employing deep learning techniques for intrusion detection, the system can effectively differentiate between legitimate and attack message packets, improving overall network security. The model includes a binary classification algorithm that helps in accurately identifying potential threats and minimizing false alarms.The paper discusses the implementation of an Intrusion Detection System (IDS) in a vehicular network using a deep learning approach. The system utilizes safety-related messages exchanged through V2V communication to enhance security and reduce the risk of cyber-attacks in the automotive network. By employing deep learning techniques for intrusion detection, the system can effectively differentiate between legitimate and attack message packets, improving overall network security. The model includes a binary classification algorithm that helps in accurately identifying potential threats and minimizing false alarms.

[4] The proposed system in the document focuses on using deep learning, specifically deep neural networks, for intrusion prevention in the Internet of Vehicles (IoV). The system aims to classify normal packets from malicious packets to enhance security in vehicular networks. It

involves preparing a training dataset from open-source datasets, preprocessing the network data using an autoencoder, filtering valuable features, training the model with structured deep neural networks, and combining it with a Softmax classifier and Relu activation functions. The model is trained and tested using Google Colab and TensorFlow, achieving a high accuracy of 99.57%. The system demonstrates improved efficiency and accuracy compared to existing models based on recurrent neural networks (RNN) and convolutional neural networks (CNN). The proposed system offers a promising approach to enhancing security in the Internet of Vehicles through deep learning techniques.

[5] The document discusses a data-driven intrusion detection system for Intelligent Internet of Vehicles (IoV) using a deep convolutional neural network (CNN) architecture. The system aims to analyze link load behaviors in IoV to detect and prevent various attacks, such as Distributed Denial of Service (DDoS) attacks and rogue nodes. The CNN is utilized to extract features from network traffic data and identify anomalies indicative of intrusions targeting Road Side Units (RSUs) in smart cities. The proposed architecture enhances the security of IoV by efficiently analyzing traffic flows and detecting malicious activities, ultimately safeguarding the integrity and functionality of the IoV ecosystem.

[6] The paper introduces an Intrusion Detection System (IDS) designed for Vehicular Networks, leveraging a deep learning approach to enhance security and safety in automotive communication systems. The system's core functionality lies in its ability to differentiate between benign and malicious data packets exchanged between vehicles and roadside devices. By utilizing deep learning techniques for binary classification, the IDS aims to identify and prevent potential cyber threats within the network. To train the model, the researchers construct a comprehensive dataset comprising network packets and features extracted from publicly available datasets such as KDD99 and CICIDS 2018. Autoencoders are employed to filter out extraneous information from the network data, ensuring that only relevant features are considered during the training process. The model is then trained using structured deep neural networks, incorporating Softmax classifiers and ReLU activation functions to optimize performance. Through rigorous experimentation and testing, the IDS achieves an impressive accuracy rate of 99.57%, surpassing existing models based on recurrent neural networks (RNN) or convolutional neural networks (CNN). The study demonstrates the efficacy of the proposed IDS in effectively detecting and preventing intrusions in Vehicular Networks, highlighting the potential of deep learning in enhancing cybersecurity measures within the automotive industry.

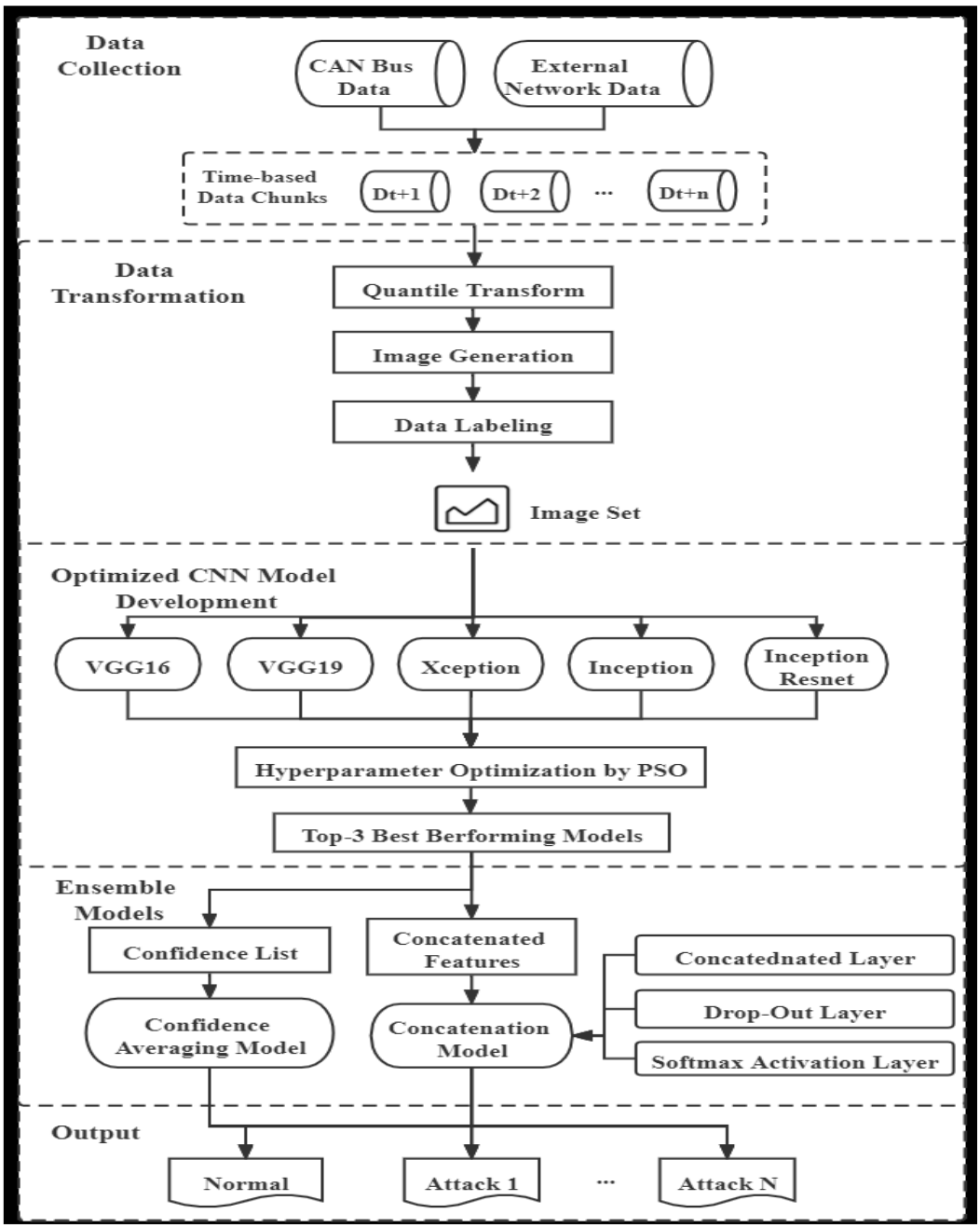
[7] The Paper discusses an Intrusion Detection System (IDS) for detecting cyberattacks in the Internet of Vehicles (IoV) environment using machine learning techniques. It addresses the challenges of identifying abnormal behavior in network traffic to detect various types of cyberattacks targeting vehicles in the IoV ecosystem. The proposed framework involves data preprocessing, feature selection, and model training using Random Forest, Extreme Gradient Boosting, Categorical Boosting, and Light Gradient Boosting Machine algorithms with hyperparameter optimization. The system aims to achieve high accuracy above 99.8% while avoiding overfitting issues. Techniques such as Synthetic Minority Oversampling Technique (SMOTE) and feature selection are employed to handle imbalanced datasets and improve model performance. The study combines datasets from CIC-IDS-2017, CSE-CIC-IDS-2018, and CIC-DDoS-2019 to build a comprehensive IDS model for detecting a wide range of cyberattacks in the IoV environment.

Proposed Work:

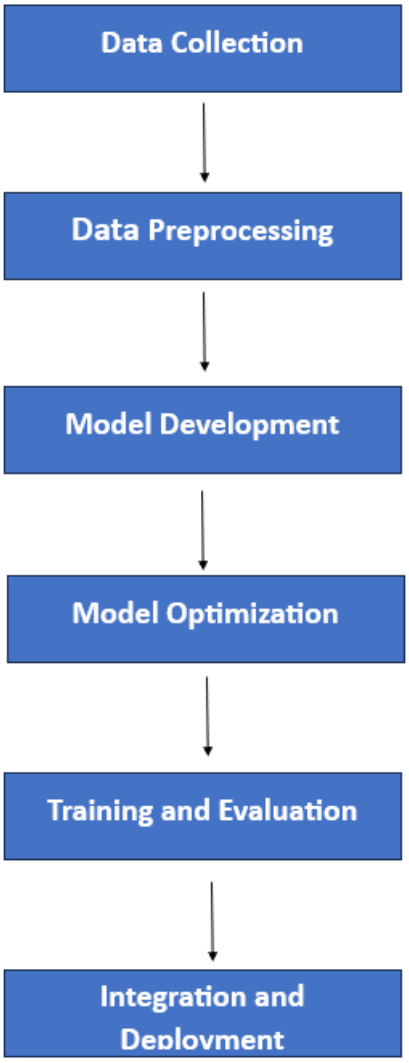
In this project, we're building a system to detect unauthorized activities in Internet-connected vehicles. We'll use a type of advanced computer program called a Convolutional Neural Network (CNN) to do this efficiently. First, we'll gather data from vehicle sensors and networks. Then, we'll design a CNN to analyze this data and spot any suspicious behavior. We'll fine-tune the CNN to make sure it works as accurately as possible. After testing, we'll integrate our system with the vehicles' internet setup for real-time monitoring. By doing this, we hope to make connected vehicles safer and more secure.

Detailed design:

Architecture Diagram



Methodology and Module Description:



1.

2.

3

Signature (Students) **Signature (Guide)**