engineering proceedings

MDPI

Proceeding Paper

Transfer Learning-Based Anomaly Detection System for Autonomous Vehicle †

Md. Humayun Kabir [1,2,*], Mohammad Nadib Hasan [1], Ahmad [3] and Hassan Jaki [1]

[1] Department of Computer and Communication Engineering, International Islamic University Chittagong, Kumira Chattogram 4318, Bangladesh; nadibhasan@iiuc.ac.bd (M.N.H.); hassanjaki11@gmail.com (H.J.)
[2] Department of Electronics and Telecommunication Engineering, Chittagong University of Engineering and Technology (CUET), Chittagong 4349, Bangladesh
[3] Department of Electronics and Telecommunication Engineering, International Islamic University Chittagong, Kumira Chattogram 4318, Bangladesh; ahmadcse0@gmail.com
* Correspondence: mdhkrrabby@gmail.com; Tel.: +880-151-528-6984
† Presented at the 10th International Electronic Conference on Sensors and Applications (ECSA-10), 15–30 November 2023; Available online: https://ecsa-10.sciforum.net/.

Abstract: The advancements in technology have brought about significant changes in the automobile industry. A system that combines the control of a physical process with computing technology and communication networks is called a cyber–physical system (CPS). The enhancement of network communication has transitioned vehicles from purely mechanical to software-controlled technologies. The controller area network (CAN) bus protocol controls the communication network of autonomous vehicles. The convergence of technologies in autonomous vehicles (AVs) and connected vehicles (CVs) within Connected and Autonomous Vehicles (CAVs) leads to improved traffic flow, enhanced safety, and increased reliability. CAVs development and deployment have gained momentum, and many companies and research organizations have announced their initiatives and begun road trials. Governments worldwide have also implemented policies to facilitate and expedite the deployment of CAVs. Nevertheless, the issue of CAV cyber security has become a prevalent concern, representing a significant challenge in deploying CAVs. This study presents an intelligent cyber threat detection system (ICTDS) for CAV that utilizes transfer learning to detect cyberattacks on physical components of autonomous vehicles through their network infrastructure. The proposed security system was tested using an autonomous vehicle network dataset. The dataset was preprocessed and used to train and evaluate various pre-trained convolutional neural networks (CNNs), such as ResNet-50, MobileNetV2, AlexNet, GoogLeNet and YOLOV8. The proposed security system demonstrated exceptional performance, as demonstrated by its results in precision, recall, F1-score, and accuracy metrics. The system achieved an accuracy rate of 99.90%, indicating its high level of performance.

Keywords: autonomous vehicles; cyber–physical system; security; cyber-attacks; transfer learning

Citation: Kabir, M.H.; Hasan, M.N.; Ahmad; Jaki, H. Transfer Learning-Based Anomaly Detection System for Autonomous Vehicle. *Eng. Proc.* **2023**, *58*, 90. https://doi.org/10.3390/ecsa-10-16248

Academic Editor: Stefano Mariani

Published: 15 November 2023

1. Introduction

The emergence of connected and autonomous vehicles represents a shift towards a transportation system that utilizes intelligent automation and robust communication to replace traditional human-operated vehicles. These vehicles are designed to operate with the same level of intelligence, control, and agility as human drivers while minimizing the potential for errors in decision-making, making it the future of transportation [1]. AVs integrate advanced vehicle technologies to enable self-driving capabilities. AVs can perform complex functions, such as lane departure alerts, identification of traffic signs, and collision avoidance, which can decrease the burden on human drivers [2]. The increasing interest in autonomous vehicles has led to a proliferation of research and development efforts in the field, with various companies and organizations investing in developing autonomous vehicle technology. Furthermore, AVs can have a positive environmental

impact by decreasing energy consumption and air pollution. These vehicles are composed of intricate systems that necessitate advanced computing, sensing, actuation, networking, and communication technologies [3].

Initially, manual vehicles require additional connectivity to the exterior, making it challenging for hackers to attack, as they would need physical access to the vehicle. The researchers could control the vehicle through wired connections, such as altering the display dashboard, shutting down the engine, and interfering with steering. With the advancement of AV technology in recent years, vehicles are equipped with various sensors to aid human driving. Figure 1 shows the overview of CAV cyberattack AV systems [4].

Figure 1. CAVs cyberattacks Holistic View.

The use of communication protocols is essential to guarantee the safety and stability of AVs. One commonly used protocol is CAN, which provides high-speed communication within the vehicle. Time-Triggered CAN (TTCAN) offers time-deterministic communication, an improvement from the basic CAN protocol. Local Interconnect Networks (LIN) connect low-cost sensors and actuators, providing a simple and economical communication solution [5]. FlexRay is a new protocol that offers high-speed and dependable communication for critical applications requiring real-time data transmission, like advanced driver assistance systems (ADASs). In autonomous vehicles, communication protocols such as CAN, TTCAN, LIN, and FlexRay are vital in addressing data transmission, real-time data analytics, bandwidth restrictions, privacy, and security [6]. The vulnerability of autonomous vehicles to security threats increases with their level of autonomy. The information from various control systems is transmitted to every node in the network through the Controller Area Network bus [7]. With data accessible to all nodes, it can expose the system to potential security risks from internal or external sources. Potential attack surfaces for AVs include the Airbag Electronic Control Unit (ECU), USB, Bluetooth, and the Vehicle Access System ECU. To ensure the safe and reliable operation of these vehicles, they must be equipped with advanced communication and sensing technology to counteract these potential threats [8].

Fully autonomous vehicles can carry out driving tasks and make instantaneous adjustments without requiring any input from the driver. The SAE has established a categorization of six levels to measure vehicle automation, taking into consideration factors such as the vehicle's ability to manage driving tasks and responses, detect objects and events, make corrections in case of system failures, and operate within specific domains. The responsibilities of the driver and the autonomous vehicle system vary with each level of automation, which can be seen in summary [9,10]:

Level 0: Driver-Only Control: At Level 0, the driver must handle all vehicle driving and control responsibilities. This includes being alert to their surroundings and responding to any events. If the system encounters any problems, it is up to the driver to fix the issue. This level does not specify any operational design domain.

Level 1: Driver Assistance: At Level 1 of automation, the vehicle is operated by collaborating with the driver and the system. The system can either control speed or direction, but not both. The driver is required to supervise the environment and respond to any situation. Additionally, if the system fails, the driver must control the vehicle. The operational design domain is also restricted to a small area at this level.

Level 2: Shared Control: At this level, the system is capable of controlling both the vertical and horizontal motions of the vehicle at the same time. However, the driver must still monitor the environment and take action if needed. In case of a system malfunction, the driver must regain vehicle control. The operational design domain is still limited at this level.

Level 3: Conditional Driving Automation: The system can control both longitudinal and lateral motion. It also monitors the environment and reacts to events and objects. If the system fails, the driver should be ready to respond to its request or take control of the vehicle. The operational design domain's extent is restricted at this level.

Level 4: Highly Automated Driving: The vehicle's system can manage both longitudinal and lateral driving tasks at the same time. The system is in charge of observing the surroundings and handling any events. If there is a system malfunction, the system must be able to recover without driver intervention. There are specific boundaries to the system's operating range at this level of automation.

Level 5: Complete Driving Automation: The vehicle can control both longitudinal and lateral driving tasks at the same time. The system is accountable for observing the environment and taking appropriate measures. In case of system failure, the vehicle's technology can recover without human intervention. This level of automation has no limitations in the operational design domain.

The vulnerability of CAVs to cyberattacks is amplified by their connectivity and autonomy capabilities when exchanging data with other vehicles and the environment. Autonomous vehicles face risks from cyberattacks such as cloning essential fobs, attacks on radars and telematics services, deception of sensors using ultrasonic or lidar technology, camera sensor attacks, and others. To counter these threats, a method has been proposed using a convolutional neural network (CNN) that has already been trained to detect cyberattacks on the connected physical parts of AVs through the CAN communication protocol. The technique employs transfer learning, a deep learning strategy that utilizes pre-trained models for various systems. This is important because it can be challenging and costly to gather enough data to train a model through traditional machine learning methods. The process of transfer learning involves adjusting a pre-trained model to a new and related model, enabling the model to learn from data from diverse domains [11,12].

This study proposes a solution for detecting cyberattacks on autonomous vehicles using a pre-trained CNN and the CAN communication protocol. The method consists of incorporating the CAN protocol into an AV simulation model that is built using Simulink from MathWorks. This model generates the dataset that is used to pre-train the CNN. The IIDS implemented uses four pre-trained networks and evaluates each network's performance. The results showed that the YOLOV8 network had the best performance, with an F1-score of 99.90%. The manuscript comprises four sections. The first part scrutinizes the latest studies on autonomous vehicle security. The second section delineates the research process, which includes integrating the AV-CPS. The third part presents the discoveries and debates, whereas the last segment concludes the paper.

2. Proposed Methodology

This study segment elaborates on the simulation methodology employed for analyzing autonomous vehicles. This section explains how the simulation of cyber–physical systems is incorporated to create the AV-CPS model shown in Figure 2. It also describes how data are collected from the AV-CPS simulation and discusses the application of this data in transfer learning.

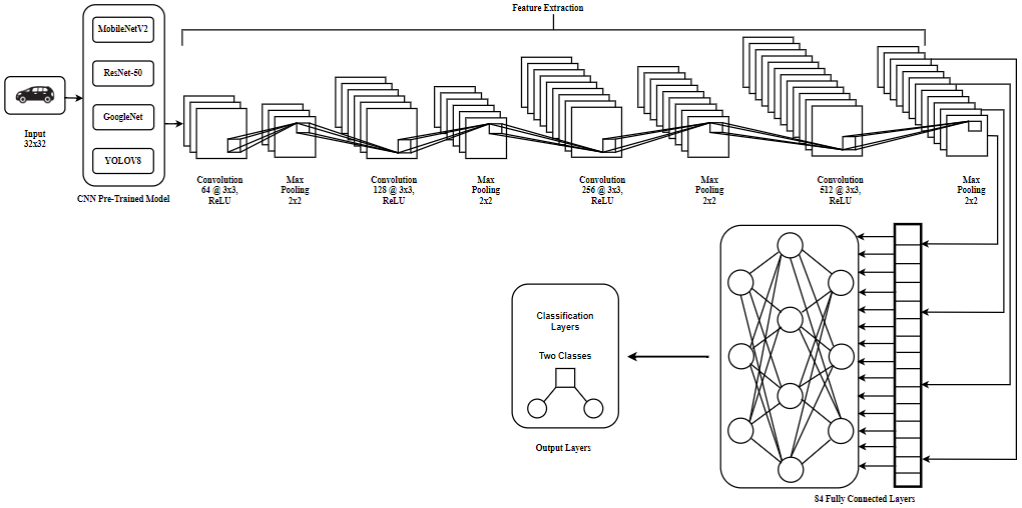

Figure 2. Architecture of the Proposed Pre-trained Models.

2.1. AV Simulation Scheme

The research employs a software-based simulation model to assess the performance of a self-driving car system before its deployment. The simulation model comprises an ego vehicle (i.e., the self-driving car) and a lead vehicle. The former utilizes an adaptive cruise controller (ACC) to maintain a safe distance from the latter while tracking its position and velocity. The simulation model integrates three crucial components: the ACC, a sensor to detect the position of both vehicles, and a sensor to record their velocity. The sensor measurements are relayed to the ACC, which subsequently regulates the speed of the vehicle in response to the movements of the lead vehicle.

2.2. CAN Communication Network

This study employed a simulation model of a self-driving car system to assess its performance before deployment. The simulation model for the AV-CPS was based on the ACC system, which consisted of an ACC, a position sensor, and a velocity sensor. However, there was no communication system component included in the model. To address this, the researchers used the Vehicle Network Toolbox on Simulink to implement a communication system based on the CAN protocol. The study focused on establishing the AV-CPS communication system using the CAN communication component to transmit and receive messages between the various elements. The signals were encapsulated and dispatched to the assigned CAN device, then received and decomposed into signals.

2.3. Autonomous Vehicle Cyber-Physical System

This study implemented an AV-CPS architecture to investigate the performance of the self-driving car system, which consisted of multiple components such as sensors, two CAN communication nodes, a controller, and actuators. The first communication node (Node A) receives and transmits signals such as the actual location, position, and speed of the ego and lead vehicles, as well as a constant time gap and desired speed. These signals are then used by the ACC to generate a control signal, which is sent to Node B. Node B then receives and transmits this control signal to the actuators, where it is converted into a mechanical movement that changes the speed of the vehicle. The entire process is repeated in a closed-loop simulation for a total of 81 s.

2.4. Generating Dataset

This research developed a cyber–physical system-based autonomous vehicle simulation, integrating a CAN communication system. The simulation model comprised a lead vehicle and a self-vehicle. The latter utilized sensors to monitor vehicles' position and velocity, maintaining a safe distance through the ACC. However, the researchers considered

a compromised communication node scenario where false data were inserted into the ego vehicle's position sensor, causing the ACC to produce erroneous control signals. The data generated by the simulation was in a numerical format and consisted of five attributes, namely, the actual position and velocity of both vehicles and an anomaly detection label.

2.5. Transfer Learning

This section details the utilization of transfer learning in the research, which involves adapting pre-trained models to improve performance on a related task. This study utilized pre-trained models such as MobileNetV2, GoogLeNet, ResNet-18, and YOLOv8, all containing layers like Relu, Pooling, and Fully connected layers to ensure accurate image classification show in 3. These models have Relu, Pooling, and Fully connected layers to improve image classification. The final layer of each model has been modified to output only normal or anomaly categories. The dataset was preprocessed to be compatible with each CNN model. During AV-CPS simulation, feature responses were stored as numerical values in a matrix, which was reshaped from 1D to 2D. The resulting 2D matrix was saved as an image, and normal/anomaly images were stored separately for analysis.

3. Results and Discussion

This section covers the specifics of the experimentation, such as the tools and equipment employed to carry out the study. Additionally, the section will present and analyze the outcomes of the research. The study utilized Matlab and Simulink for experiments. Matlab is a programming language platform, whereas Simulink is a design platform based on Matlab. The AV simulation model was created using both Matlab and Simulink by MathWorks. The researchers used the Simulink network toolbox to integrate the CAN protocol component into the AV simulation. Matlab was used for implementing and evaluating pre-trained CNNs. A computer with a GPU was utilized for experiments to enhance performance and reduce computation time.

Figure 3 displays the overall steps taken in this research's experiments. The initial stage involved importing a dataset into Matlab. The images were preprocessed by resizing them to comply with the input size requirements of pre-trained CNNs programmed to classify images as either normal or anomalous. The dataset contained two folders, one with normal images and the other with anomalous images. It was split into 70% for training and 30% for testing and validation. The dataset included 20,000 images, half normal and the other half anomalous. To ensure the training process's accuracy, a 5-fold cross-validation technique was employed, and the expected output of each model was either normal, indicating no attack, or anomalous, indicating that an attack had occurred.

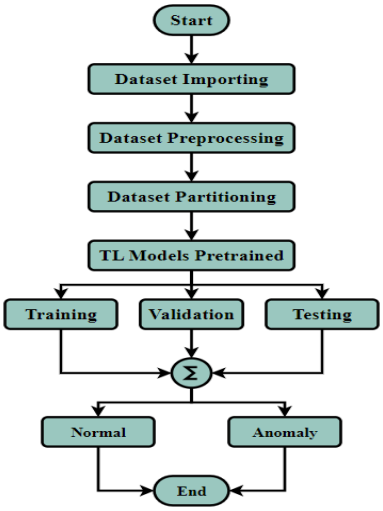

Figure 3. Research Experiment Steps.

The study evaluated pre-trained CNN model performance using several metrics, including precision, recall, F1-score, and accuracy classification. The accuracy of the models was determined by calculating true positive (TP), false positive (FP), false negative (FN), and true negative (TN). Table 1 displays the accuracy of the models, with YOLOV8 performing the best. Although all models had 100% precision, recall values ranged from 98.65% to 99.00%, indicating the misclassification of some anomalous images as normal.

Table 1. Performance Comparison of Pre-trained Model Accuracy.

Pre-Trained Model	Precision	Recall	F1 Score	Accuracy
ResNet-50	100%	98.86%	99.40%	99.40%
MobileNetV2	100%	98.65%	99.35%	99.35%
AlexNet	100%	98.90%	99.45%	99.45%
GoogLeNet	100%	98.96%	99.50%	99.50%
YOLOV8	100%	99.00%	99.90%	99.90%

To substantiate our findings, we conducted a comparative analysis of the performance outcomes of our research about existing intrusion detection system approaches employed in autonomous vehicle systems. In general, pre-trained convolutional neural networks, such as those discussed in research papers like ResNet-50, MobileNetV2, AlexNet, GoogLeNet, and YOLOV8, exhibited superior performance compared to alternative models, such as artificial neural networks (ANN) and Bayesian networks, as indicated in Table 1.

4. Conclusions

The research proposed an IIDS that uses the CAN to identify cyberattacks on the physical components of AVs. The CAN was included in an AV simulation by MathWorks to illustrate the CPS concept, resulting in an AV-CPS. The AV-CPS created the dataset, which was transformed into images and inputted into pre-trained CNNs such as ResNet-50, MobileNetV2, AlexNet, GoogLeNet, and YOLOV8. The performance of each network was assessed and compared, and YOLOV8 had the best performance, with an F1 score of 99.90%. The proposed system's block architecture makes it adaptable and resilient to other CPS frameworks. The study suggested extending the AV-CPS system architecture to other CPS domains such as smart grids and drones.

Author Contributions: Conceptualization, M.H.K. and M.N.H.; methodology, M.H.K. and A.; software, M.N.H., H.J., A. and M.H.K.; formal analysis, M.H.K., M.N.H., A. and H.J.; writing—original draft preparation, M.H.K. and M.N.H.; writing—review and editing, M.H.K., A. and M.N.H.; supervision, M.H.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Park, K.J.; Zheng, R.; Liu, X. Cyber-physical systems: Milestones and research challenges. *Comput. Commun.* **2012**, *36*, 1–7. [CrossRef]
2. Rajkumar, R.; Lee, I.; Sha, L.; Stankovic, J. Cyber-physical systems: The next computing revolution. In Proceedings of the 47th Design Automation Conference, Anaheim, CA, USA, 13–18 June 2010.
3. Kim, S.; Park, K.-J. A Survey on Machine-Learning Based Security Design for Cyber-Physical Systems. *Appl. Sci.* **2021**, *11*, 5458. [CrossRef]

4. Aldhyani, T.H.H.; Alkahtani, H. Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity. *Sensors* **2022**, *22*, 360. [CrossRef] [PubMed]
5. Wang, Z.; Wei, H.; Wang, J.; Zeng, X.; Chang, Y. Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey. *Sustainability* **2022**, *14*, 12409. [CrossRef]
6. NHTSA. SAE Define 5 Levels of Vehicle Automation. Available online: https://www.sema.org/sema-enews/2017/11/ettn-tech-alert-nhtsa-sae-define-5-levels-of-vehicle-automation (accessed on 19 October 2023).
7. Petit, J.; Shladover, S.E. Potential cyberattacks on automated vehicles. *IEEE Trans. Intell. Transp. Syst.* **2014**, *16*, 546–556. [CrossRef]
8. Parkinson, S.; Ward, P.; Wilson, K.; Miller, J. Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2898–2915. [CrossRef]
9. Lokman, S.F.; Othman, A.T.; Abu-Bakar, M.H. Intrusion detection system for automotive Controller Area Network (CAN) bus system: A review. *EURASIP J. Wirel. Commun. Netw.* **2019**, *2019*, 184. [CrossRef]
10. Young, C.; Zambreno, J.; Olufowobi, H.; Bloom, G. Survey of automotive controller area network intrusion detection systems. *IEEE Des. Test* **2019**, *36*, 48–55. [CrossRef]
11. Cao, Y.; Xiao, C.; Cyr, B.; Zhou, Y.; Park, W.; Rampazzi, S.; Chen, Q.A.; Fu, K.; Mao, Z.M. Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), London, UK, 11–15 November 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 2267–2281. [CrossRef]
12. Stottelaar, B.G. Practical Cyber-Attacks on Autonomous Vehicles. Master's Thesis, University of Twente, Enschede, The Netherlands, 2015.