AN APPROACH FOR VEHICLE INTRUSION DETECTION USING EXTREME LEARNING MACHINE -NOVEL CONVOLUTION NEURAL NETWORK MODEL COMPARED OVER SUPPORT VECTOR MACHINE ACCURACY

S. Bhaskara Rao M[1] P. V. Pramila M[2*]

Article History: Received: 12.12.2022 **Revised:** 29.01.2023 **Accepted:** 15.03.2023

Abstract

Aim: The main objective of the Vehicular Intrusion detection system is to improve the safety of wireless vehicular communication efficiency and waiting time on the road using the algorithms in Machine Learning.
Methods and Materials: The categorizing is performed by adopting a sample size of N=20 in Convolutional Neural Neural Network (N=20) and a sample size of N=20 in Support Vector Machine algorithms**.** The dataset is collected from www.kaggle.com.
Result: The Support vector machine recognized the intrusion in the CAN bus with 85% accuracy while for the Novel Convolution Neural Networks it was 95%. The independent significant value p=0.442 ($p<0.05$) showed that there is no significant difference between the two models considered.
Conclusion: Recognizing In-Vehicle Network Intrusion significantly seems to be better in Novel Convolution Neural Network (CNN) than Support Vector Machine.

Keywords: Vehicle intrusion, Novel Convolution Neural Network, CAN Bus, Support vector machine, Machine Learning.

[1]Research Scholar, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamil Nadu, India, 602105.
[2*]Project Guide, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences Saveetha University, Chennai, Tamil Nadu, India, 602105.

1. Introduction

In the past few years Intelligent vehicles have been developed as a result of technological advancements, and are thought to be more efficient and safer for users. Intelligent vehicles are typically linked to other vehicles, roadside infrastructure, such as traffic control systems, and the internet, putting them in the Internet of Things category(Mayr et al. 2007). However, because of their high levels of connectivity, intelligent vehicles are vulnerable to cyber-attacks that could disrupt many components of the vehicle, such as communication systems, endangering the vehicle's security and privacy as well as threatening the lives of its occupants to produce Can Bus packets.

Vehicle Intrusion can be carried out from the researchers.There are 108 articles found on IEEE, and 564 articles were found in the Google Scholar. The goal of connected vehicle technology has always been to solve the problems that intelligent transportation systems can face. Intelligent vehicles can usually connect with roadside infrastructure, other vehicles on the road, and other road users through an Intelligent Transport System(Agarap 2018; Ahmad et al. 2018). The communication system of an Extreme Learning Machine of intelligent vehicle is usually referred to as Vehicle-to-Everything (V2X) or it is also referred to as the VANET, an abbreviation for Vehicular Ad hoc Networks (Mirjalili, Faris, and Aljarah 2019). To be classified as smart automotive, a typical VANET communication system is usually responsible for three main types of communication. Vehicle-to-Infrastructure (V2I), Vehicle-to-Vehicle (V2V), and Vehicle-to-Pedestrian (V2P) are the three types of communication Vehicle-to-infrastructure communication (V2I) includes the vehicle communicating with roadside infrastructures such as location sensors and other traffic monitoring systems. V2V refers to a smart car's ability to share data with other vehicles on the road.

Our team has extensive knowledge and research experience that has translated into high quality publications (K. Mohan et al. 2022; Vivek et al. 2022; Sathish et al. 2022; Kotteeswaran et al. 2022; Yaashikaa, Keerthana Devi, and Senthil Kumar 2022; Yaashikaa, Senthil Kumar, and Karishma 2022; Saravanan et al. 2022; Jayabal et al. 2022; Krishnan et al. 2022; Jayakodi et al. 2022; H. Mohan et al. 2022). (Greenberg 2019) established a few crafted messages in the structure of CAN Bus packets that were sent remotely in the form of messages. As a result, some of the car's essential issues like the braking machine were once disabled ((Mirjalili, Faris, and Aljarah 2019)). As well, the steering wheel became 180° while the passenger was driving in traffic.(Greenberg 2019; Bazi and Pasolli 2021) implemented a secure gateways that gives the secure access from installed applications in the internal vehicle system.(Mirjalili, Faris, and Aljarah 2019) a very lightweight algorithm based on the observance of CAN packet frequencies stimulated from They simplified the detection algorithm so that it may want to react quicker to the intrusion while, at the same time, computing power utilization can be reduced (Mirjalili, Faris, and Aljarah 2019).

2. Methods and Materials

The study setting of the proposed work was done in the Object Oriented Analysis And Design laboratory at Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences The sample size was calculated by using clincalc.com by keeping G power, minimum power of the analysis fixed as 0.8 and 0.5 respectively with threshold value as 0.05%.. The two groups are used namely Novel Convolution Neural Network(N=20) as an existing model as group 1 and Support Vector Machine(N=20) as a Proposed model as group 2.

Novel Convolution Neural NetworkS (CNN)
The typical model of CNN has a single input and output layer along with multiple hidden layers. A particular neuron takes input vector X and produces output Y by performing some function F. The CNN model differentiate one from the other. It can produce highly abstract features and can identify objects efficiently and it is represented by general equation (1) shown below.

$$F(X,W) = Y \quad (1)$$

Pseudo Code
Step 1. Import the dataset.
Step 2. preprocess the imported data.
Step 3. Select the classification and tokenize the data.
Step 4. Computing term frequency and creating document term matrix.
Step 5. Evaluating the data by using an evaluation algorithm.

Support Vector Machine (Svm)
SVM could be a supervised machine learning formula, and it is used for either classification or regression challenges. However, it's largely utilized in classification issues. Therefore, there area unit several applications of SVM like in E-commerce,

Stock promoting, etc. Not like different machine learning algorithms, SVM relies on the conception of call planes that defines call boundaries. It is a kind of graphical approach. shows the steps in the below implementation.

Pseudo Code
Step 1. Import the dataset.
Step 2. preprocess the imported data.
Step 3. Select the classification and tokenize the data.
Step 4. Computing term frequency and creating document term matrix.
Step 5. Evaluating the data by using an evaluation algorithm.
For comparing both the models, the dataset has been trained with five different sample sizes. the accuracy values are recorded. The system configuration is used for the algorithm to run in a 64 - bit Operating System, 4GB RAM PC, and using Windows 10, Google Colab, and Microsoft Office for software specification.

Statistical analysis
The IBM SPSS version 21 statistical software is used for our study. The independent variables are shape and size and the dependent variable is accuracy (%). for our study Intrusion detection. In SPSS, the datasets are prepared using N=10 as the sample size for Convolution Neural Network and Support Vector Machine. GroupID is given as a grouping variable and accuracy is given as the testing variable. GroupID is given as 1 for Convolutional Neural Network and group 2 for SVM. Group Statistics is applied for the Statistical Package for the Social Sciences (SPSS) dataset and shown in Table 2. By performing the statistical analysis group statistics represents the comparison of the accuracy and Loss of Vehicle Intrusion detection of Convolutional Neural Network and SVM. The Convolutional Neural Network had the highest accuracy (95%) . SVM had the lowest accuracy (85%) in Table 2. Accuracy for Convolutional Neural Network and Support Vector Machine algorithms have been calculated primarily based on equation(2)

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad \ldots\ldots\ldots(2)$$

where,

TP, is the number of true positives classified by the model
TN, is the number of true negatives classified by the model
FP, is the number of false positives classified by the model
FN, is the number of false negatives classified by the model

3. Results

Table 2, shows the results of proposed algorithm Novel Convolution Neural Network and the existing system Support Vector Machine Algorithm where the accuracy of CNN, is taken as N=20 iterations and mean value obtained is 94.5070 and standard deviation and standard error mean is 2.32248,0.73443. Group of SVM is N=20 iterations and Mean value obtained is 84.2440, standard deviation and standard error mean is 0.63745, 0.20158. It was observed that the mean accuracy of the CNN algorithm was 95% and the Support Vector algorithm was 85%. Table 3, shows the accuracy level of Equal variances assumed in Levene's Test for equality of variances of F value obtained is 20.250 and Sig value is 0.442 and T-Test for equality of means t is 9.537 and df value 183 and Sig.(2-tailed) is 0.442 and Mean Difference and Standard error difference is7.26300, 0.7616 and 95% Confidence Interval of the Difference of Lower is 5.66295 and Upper is 8.86305. An one more accuracy equal variances not assumed and T-Test for equality of means t is 9.537 and df is 10.34 and Sig.(2-tailed) one sided p is 0.001 and Mean Difference and standard error difference is 5.57377, 0.76160 and 95% confidence interval of the difference of Lower is 5.57377 and Upper value is 8.95223. The Independent Sample T-Test that is applied for the sample collections by fixing the level of significance as 0.442 with a confidence interval of 95 %. After applying the SPSS calculation, SVM has accepted a statistically significant value($P<0.05$). From Figure 1 it was represented by a simple bar Mean of Accuracy Novel Convolution Neural Network error range (0.99 - 0.98) and SVM error range (0.99 - 0.98).

From Fig.1, shows mean accuracy between Simple Novel Convolutional Neural Network and Support Vector Machine Algorithm. From the results, it is shown that connected components are appearing at higher value.The comparison bar graph shows that Novel Convolution Neural Network is higher.

4. Discussions

CNN and support vector machine algorithms are applied and compared to security vehicle intrusion to enhance the accuracy by connected vehicles. From obtained results it is concluded that the Novel Residual Neural Network algorithm gives higher accuracy of 99% with significance of 0.0001 as compared to the SVM algorithm. The Deep Learning model of Convolution Neural

Network algorithm is a promising option for Vehicular Intrusion (Alazab and Tang 2019). In a short period of time a more accurate model will come by using those tools would signify that substantially and general outcomes show that there are a few varieties seen in vehicular intrusion detection by using these algorithms(Khammassi and Krichen, n.d.). (Han, Kwak, and Kim 2018) demonstrated experimental recall accuracy of 92% that enables the vehicle to self-check the vehicle condition, and can promptly provide a driver with information needed to make decisions. The Neural Networks with a precision of 90 % is superior to the Support vector Machine with an exactness of 85% in perceiving the intrusion (Alazab and Tang 2019). (Li et al. 2022) reported the average detection rate of the KNN algorithm was 84.31 percent and that of the AdaBoost algorithm was 85.06 percent. (Hu et al. 2022) showed in their work that the Mosaic coding approach has greater classification ability of 92% while confronting various sorts of attacks with significantly lower variance in all evaluation indices.

5. Conclusion

The accuracy rate of the Novel Convolution Neural Network algorithm has been improved (95%) & Support Vector Machine, which is having (85%). By comparing both algorithms, the Novel Convolution Neural Network algorithm has high accuracy.

Declarations

Conflict of interests

No conflicts of interest in this manuscript.

Authors Contributions

Author SBR was involved in conceptualization, data collection, data analysis, manuscript writing. Author PVP was involved in conceptualization, guidance, and critical review of the manuscript.

Acknowledgments

The authors would like to express their gratitude towards Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (Formerly known as Saveetha University) for providing the necessary infrastructure to carry out this work successfully.

Funding

We thank the following organizations for providing financial support that enabled us to complete the study.

1.SNEW.AI Technologies, Hyderabad

2. Saveetha University

3. Saveetha Institute of Medical and Technical Sciences.

4. Saveetha School of Engineering

6. References

Agarap, Abien Fred M. 2018. "A Neural Network Architecture Combining Gated Recurrent Unit (GRU) and Support Vector Machine (SVM) for Intrusion Detection in Network Traffic Data." Proceedings of the 2018 10th International Conference on Machine Learning and Computing. https://doi.org/10.1145/3195106.3195117.

Ahmad, Iftikhar, Mohammad Basheri, Muhammad Javed Iqbal, and Aneel Rahim. 2018. "Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection." IEEE Access. https://doi.org/10.1109/access.2018.2841987.

Alazab, Mamoun, and Mingjian Tang. 2019. Deep Learning Applications for Cyber Security. Springer.

Bazi, Yakoub, and Edoardo Pasolli. 2021. Advanced Deep Learning Strategies for the Analysis of Remote Sensing Images. MDPI.

Greenberg, Andy. 2019. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. Anchor.

Han, Mee Lan, Byung Il Kwak, and Huy Kang Kim. 2018. "Anomaly Intrusion Detection Method for Vehicular Networks Based on Survival Analysis." Vehicular Communications. https://doi.org/10.1016/j.vehcom.2018.09.004.

Hu, Rong, Zhongying Wu, Yong Xu, and Taotao Lai. 2022. "Multi-Attack and Multi-Classification Intrusion Detection for Vehicle-Mounted Networks Based on Mosaic-Coded Convolutional Neural Network." Scientific Reports 12 (1): 6295.

Jayabal, Ravikumar, Sekar Subramani, Damodharan Dillikannan, Yuvarajan Devarajan, Lakshmanan Thangavelu, Mukilarasan Nedunchezhiyan, Gopal Kaliyaperumal, and Melvin Victor De Poures. 2022. "Multi-Objective Optimization of Performance and Emission Characteristics of a CRDI Diesel Engine Fueled with Sapota Methyl Ester/diesel Blends." Energy. https://doi.org/10.1016/j.energy.2022.123709.

Jayakodi, Santhoshkumar, Rajeshkumar Shanmugam, Bader O. Almutairi, Mikhlid H. Almutairi, Shahid Mahboob, M. R. Kavipriya, Ramesh Gandusekar, Marcello Nicoletti, and Marimuthu Govindarajan. 2022. "Azadirachta Indica-Wrapped Copper Oxide Nanoparticles

as a Novel Functional Material in Cardiomyocyte Cells: An Ecotoxicity Assessment on the Embryonic Development of Danio Rerio." Environmental Research 212 (Pt A): 113153.

Khammassi, Chaouki, and Saoussen Krichen. n.d. A GA-LR Wrapper Approach for Feature Selection in Network Intrusion Detection. Infinite Study.

Kotteeswaran, C., Indrajit Patra, Regonda Nagaraju, D. Sungeetha, Bapayya Naidu Kommula, Yousef Methkal Abd Algani, S. Murugavalli, and B. Kiran Bala. 2022. "Autonomous Detection of Malevolent Nodes Using Secure Heterogeneous Cluster Protocol." Computers and Electrical Engineering. https://doi.org/10.1016/j.compeleceng.2022.107902.

Krishnan, Anbarasu, Duraisami Dhamodharan, Thanigaivel Sundaram, Vickram Sundaram, and Hun-Soo Byun. 2022. "Computational Discovery of Novel Human LMTK3 Inhibitors by High Throughput Virtual Screening Using NCI Database." Korean Journal of Chemical Engineering. https://doi.org/10.1007/s11814-022-1120-5.

Li, Zhongwei, Wenqi Jiang, Xiaosheng Liu, Kai Tan, Xianji Jin, and Ming Yang. 2022. "GAN Model Using Field Fuzz Mutation for in-Vehicle CAN Bus Intrusion Detection." Mathematical Biosciences and Engineering: MBE 19 (7): 6996–7018.

Mayr, Susanne, Edgar Erdfelder, Axel Buchner, and Franz Faul. 2007. "A Short Tutorial of GPower." Tutorials in Quantitative Methods for Psychology. https://doi.org/10.20982/tqmp.03.2.p051.

Mirjalili, Seyedali, Hossam Faris, and Ibrahim Aljarah. 2019. Evolutionary Machine Learning Techniques: Algorithms and Applications. Springer Nature.

Mohan, Harshavardhan, Sethumathavan Vadivel, Se-Won Lee, Jeong-Muk Lim, Nanh Lovanh, Yool-Jin Park, Taeho Shin, Kamala-Kannan Seralathan, and Byung-Taek Oh. 2022. "Improved Visible-Light-Driven Photocatalytic Removal of Bisphenol A Using V2O5/WO3 Decorated over Zeolite: Degradation Mechanism and Toxicity." Environmental Research. https://doi.org/10.1016/j.envres.2022.113136.

Mohan, Kannan, Abirami Ramu Ganesan, P. N. Ezhilarasi, Kiran Kumar Kondamareddy, Durairaj Karthick Rajan, Palanivel Sathishkumar, Jayakumar Rajarajeswaran, and Lorenza Conterno. 2022. "Green and Eco-Friendly Approaches for the Extraction of Chitin and Chitosan: A Review." Carbohydrate Polymers 287 (July): 119349.

Saravanan, A., P. Senthil Kumar, B. Ramesh, and S. Srinivasan. 2022. "Removal of Toxic Heavy Metals Using Genetically Engineered Microbes: Molecular Tools, Risk Assessment and Management Strategies." Chemosphere 298 (July): 134341.

Sathish, T., R. Saravanan, V. Vijayan, and S. Dinesh Kumar. 2022. "Investigations on Influences of MWCNT Composite Membranes in Oil Refineries Waste Water Treatment with Taguchi Route." Chemosphere 298 (July): 134265.

Vivek, J., T. Maridurai, K. Anton Savio Lewise, R. Pandiyarajan, and K. Chandrasekaran. 2022. "Recast Layer Thickness and Residual Stress Analysis for EDD AA8011/h-BN/B4C Composites Using Cryogenically Treated SiC and CFRP Powder-Added Kerosene." Arabian Journal for Science and Engineering. https://doi.org/10.1007/s13369-022-06636-5.

Yaashikaa, P. R., M. Keerthana Devi, and P. Senthil Kumar. 2022. "Algal Biofuels: Technological Perspective on Cultivation, Fuel Extraction and Engineering Genetic Pathway for Enhancing Productivity." Fuel. https://doi.org/10.1016/j.fuel.2022.123814.

Yaashikaa, P. R., P. Senthil Kumar, and S. Karishma. 2022. "Review on Biopolymers and Composites – Evolving Material as Adsorbents in Removal of Environmental Pollutants." Environmental Research. https://doi.org/10.1016/j.envres.2022.113114.

Tables and Figures

Table 1. Data collection from the N=10 samples of the dataset for Convolution Neural Networks to gain accuracy (%) and SVM to gain accuracy(%).

Samples(N)	**Convolution Neural Networks(CNN)**	**Support Vector Machine(SVM)**
	Accuracy(%)	**Accuracy(%)**

1	95.00	85.00
2	94.45	84.65
3	93.50	84.78
4	92.78	84.76
5	91.78	84.00
6	90.50	83.87
7	89.79	84.12
8	88.98	83.79
9	88.64	82.89
10	89.65	84.58

Table 2. Comparison of the accuracy of Intrusion Recognition of Convolution Neural Networks and SVM .Convolution Neural Network algorithm had the highest accuracy (95%). Support Vector Machine had the lowest accuracy (85%) as compared to Convolution Neural Network.

GROUP	N	Mean	Std Deviation	Std Error Mean
CNN	10	94.5070	2 .32248	.73443
SVM	10	84.2440	.63745	.20158

Table 3. Independent Sample T-Test is applied for the sample collections by fixing the level of significance as 0.05 with confidence interval as 95 %. After applying the SPSS calculation, SVM has accepted a statistically significant value($p<0.05$).

ACCURACY	**Levene's Test for Equality of Variance**		**T-test for Equality of Means**						
	f	**Sig**	**t**	**df.**	**Significanance**		**Mean Difference**	**Std.Error Difference**	**95% Confidence of the Differences**
									Lower / **Upper**
Equal variances assumed	20.25	0.442	9.537	183	One Sided p: 0.001	Two Sided p: 0.001	7.263	0.761	5.662 / 8.863

Equal variances not assumed			9.537	10.348	0.001	0.001	7.263	0.761	5.573	8.952

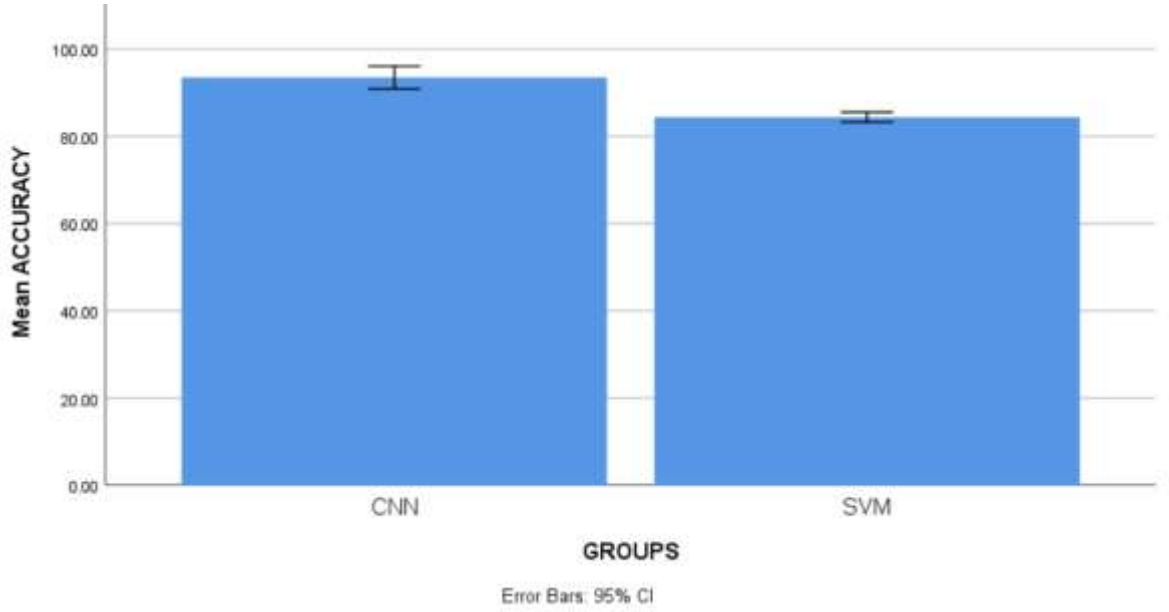

Fig 1. Simple Bar Mean of Accuracy CNN error range (0.99 - 0.98) and Loss error range (2-4) and SVM error range (0.98 - 0.99) and for loss error range (0.2-0.3) with Mean accuracy of detection ± 2 SD.X Axis: CNN vs SVM Y-Axis: Mean accuracy of detection ± 2 SD