Intrusion Detection System Using Machine Learning

AKASH BHARDWAJ[1], Dr. S S Nagamuthu Krishnan [2]
Dept. of MCA, RV College of Engineering®, Bengaluru, Karnataka, India
akashb.mca21@rvce.edu.in [1]
ssnk@rvce.edu.in [2]

Abstract

Autonomous cars (AVs) are subject to cyber assaults, include interruption of assistance, spoofing, and sniffer assaults. To tackle these weaknesses, this work offers a smart intrusion detection system, or IDS, built around tree-structure neural network models. The Intrusion Detection Systems provides high rates of detection and low rates of false alarms concurrently by combining ensemble learning with feature selection algorithms. The efficiency of the IDS is validated on common datasets, proving its capabilities to recognize different cyber assaults in AV networks. The suggested system is a noteworthy addition to the area of AV security and may be evaluated for paper publication owing to its new approach and promising outcomes.

Keywords: IDS, machine learning, cyber security, detection precision,

Introduction

This study focuses on tackling the critical problem with network risks in self-driving cars (AVs for short and presents a smart intrusion detection system, or IDS, that can effectively detect and neutralize future assaults. AVs are particularly susceptible to numerous forms of network assaults that might jeopardize human life. The article defines and covers typical forms of attack include denial services (DoS), brute-force assaults, sniffing threats such as port scanning assaults, and online attacks including SQL injections and cross-site scripting. In addition to the external communication risks, the study underlines the sensitivity of autonomous vehicles to intra-vehicle communication assaults, notably via the controller-area network (CAN) bus. Attackers may exploit the flaw by introducing fraudulent messages into the may bus, enabling attackers to monitor network activity, conduct hostile assaults, or offer misleading information.

To address these weaknesses, an intelligent IDS is developed, employing tree-based machine learning methods like choice trees, random forests, additional vegetation, and Extended Gradient Boosting (XGBoost). The IDS is intended to identify attacks that target the CAN bus system of AVs and generic Internet of Automobiles (IoT) networking. To boost accuracy, ensemble learning approaches, notably the stacking method, are applied. Additionally, feature selection approaches are applied to minimize computing time while retaining good detection.

Testing of the suggested IDS is undertaken using typical open-source datasets, confirming its excellent accuracy in spotting network intrusions. The complete approach given in this study leads to the creation of an efficient intrusion detection system for Av and general network settings. Furthermore, the adoption of an average feature selection approach boosts the performance of the IDS, allowing networks feature research and network monitoring.

Literature Survey

The literature evaluation comprised a thorough collection of data from numerous publications and conferences. The chosen papers are grouped as follows:

[1] The recognition and detection of suspicious activity are vital for network safety, and intrusion detection devices (IDS) play a critical role in this respect. It is a frequent practice to increase IDS performance by utilizing machine learning methods such as the XGBoost and Random Forests.

[2] The relevance of network safety and the crucial function of IDS (intrusion detection system) in securing network systems are underlined. The project focuses on boosting IDS accuracy by examining the usefulness of machine learning methods for intrusion detection.

[3] This work effectively integrates attack identification and mitigation into a successful framework by building a safeguarding script that performs suitable actions depending on categorization findings. The combination of attack identification and mitigation proved to be extremely successful.

[4] The study presents a complete discussion of several ways to develop effective IDS utilizing unattached, hybrid, and ensemble algorithms for learning classifiers. It covers the merits and drawbacks of each strategy, leading to the growth of IDS development.

[5] A complete review of alternative methodologies employing unattached, hybrid form, and ensemble algorithmic classifiers for generating effective IDS is provided. This investigation gives useful insights into the varied approaches applied in the building of strong IDS.

[6] Experimental findings reveal that the suggested technique using a Convolutional Neural Network, provides excellent precision for prediction, with a remarkable overall precision rate of 97.53% on many samples. This illustrates the usefulness of the suggested technique for intrusion detection.

[7] The experimental data demonstrate that the proposed technique outperforms typical machine learning techniques with regard to detection precision despite employing decreased feature vectors. The assessment is undertaken with the UNSW-NB and AWID malware detection data sets, providing empirical proof for the edge of the suggested technique.

[8] This article offers a unique deep random neural-based strategy for detecting breaches in IoT systems. The suggested scheme achieves an extraordinary efficiency of 99.54% in categorising nine distinct kinds of attacks using the UNSW-NB15 data set, exhibiting the remarkable performance of the suggested technique in the setting of IoT security.

[9] The study provides a new technique based on Boundary machine learning (ML) and meticulously evaluates the performance of machine learning (ML) algorithms on the oneM2M dataset. The research attempts to determine the best practical techniques for the Intrusion Identification and Protection System (IDPS), addressing the limits imposed by small IoT devices, including feature reduction in dimension and model size.

[10] The major goal of this research is to assess machine learning techniques for detecting intrusions using the NSLKDD database. Recursive removal of features (RFE) is performed for choosing features to boost speed and accuracy. The research includes a comparative comparison of the efficiency of random forest learning and SVM (Support Vector Machine) models prior to and following feature selection, along by a thorough explanation of confusion matrices.

Sl no	Title	Author	Success Rate
1	System for detecting invasions using machine learning	Anish Halimaa A., K.Sund-arakantham	95%
2	Using ML Approaches for Intrusion Recognition and Mitigation in Networks	Jitti Annie Abraham	92%
3	Machine Learning-Driven Network-Based Solution for Security Measures.	Hong, Chao et al	98%
4	Machine learning approaches are utilized in the development of a system to detect intrusions.	Mandeep Kaur.	96%
5	Smart Intrusion Detection Systems Using Deep Learning	Mamoun Alzab	91%
6	Convolutional neuronal is employed to detect network breaches in cyber threats.	Wen-Hui Lin	93%
7	A Machine learning methodology that leverages feature extraction approaches for wireless	Yanxia Sun	97%

	detection of intrusions utilizing wrapper-based methodologies.		
8	(IoT) systems constructed using a deep randomised neural network, proving its efficiency in identifying and avoiding breaches.	Zeba Idrees	94%
9	A benefit of OneM2M is a malware detection and Mitigation is that machine learning improves the system as a whole	Akka Zemmari	96%

Proposed Methodology

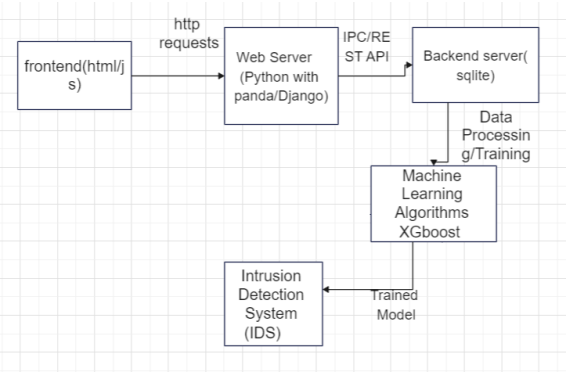

Fig1:Architectural Diagram

Architecture Diagram of Intrusion Detection

The proposed IDS demonstrates important qualities and components needed for its performance. It displays the capability to identify a broad variety of typical threats attacking both external connections and the CAN bus. The IDS provides excellent detection rates, guaranteeing rapid and precise identification of most threats, while preserving minimal computing time for better efficiency.

a) Data collection:

To assess the proposed IDS, two distinct datasets are gathered for intra-vehicle and outside-network situations. The IDS's success depends on obtaining a high rate of detection to reliably identify threats, paired with efficient computing time for better efficiency.

b) ML approaches:

Machine learning (ML) approaches are applied to handle the multi-classification difficulty of classifying distinct cyber threats. The choice tree, random forest, additional trees, and the XGBoost forest-based ML algorithms are picked for their performance in classification problems.

c) Ensemble training and features selection:

Ensemble learning employing the stacking technique is applied to further boost the IDS's accuracy. Stacking comprises a two-layer strategy where taught base predictors in the first layer feed inputs to a meta-learner in the second layer, generating a robust classifier. The four tree-based methods serve as the foundation models in the first layer, with the approach demonstrating the best accuracy chosen as the meta-classifier in the second layer.

d) Validation metrics: The suggested models are assessed using 5 subsets of the data and five times cross-validation. Various validation measures including precision, detection rates/recall, false alarm percentage, and F1 score are applied to completely assess the IDS's effectiveness, considering both proper classifications and its capacity to identify assaults correctly. Given the possible class inequalities in the databases, the detection rate measure becomes especially critical in assessing the system's capabilities to reliably identify assaults.

e). Model Training:

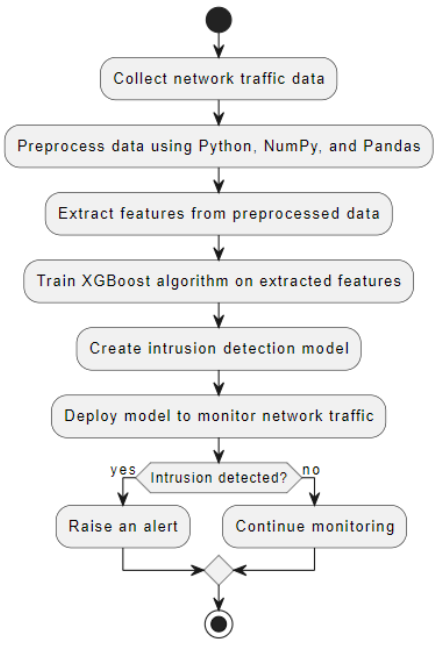

Fig2: Model Training of project

On a PC that has a 6 Quad i7-8700 Processor and 16 GB of RAM, the suggested smart IDS (intrusion detection system) is constructed using Python 3.5. The tree-based algorithm for machine learning (ML) methods takes advantage of multi-threading, providing faster performance compared to other approaches like KNN and SVM. The random forest (RF) technique, selected to serve as a meta-classifier for the stacking ensemble, displays superior accuracy and time to execution compared to the tree-based machine learning (ML) models. In addition, a feature selection tackle is utilized to minimize calculation time while retaining accuracy.

Conclusion

This paper presents an intelligent intrusion detection system, or I for autonomous vehicles, or AV utilizing tree-structure algorithms for learning models. The IDS successfully detects or mitigates network breaches across the CAN bus inside the vehicle or external networks. Ensemble learning methodologies, along with tree-based learning computations, boost the IDS's detection precision. Feature selection approaches enhance computing efficiency without losing effectiveness. The suggested IDS displays acceptable detection rates and inexpensive processing costs when assessed on typical datasets. This technology helps to enhance safety in linked and self-driving cars by delivering successful intrusion detection solutions for AV and mainstream network settings.

References

[1] A. Awang, K. Husain, N. Kamel, and S. A. Aissa, "Routing in Vehicular Ad-hoc Networks: A Survey on Single- and Cross-Layer Design Techniques, and Perspectives," IEEE Access, vol. 5, pp. 9497-9517, 2017.

[2] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun, "An overview of Internet of Vehicles," China Community, vol. 11, no. 10, pp. 1–15, 2014.

[3] K. M. Ali Alheeti and K. Mc Donald-Maier, "Intelligent intrusion detection in external communication systems for autonomous vehicles," Systems Science and Control Engineering, vol. 6, no. 1, pp. 48–56, 2018.

[4] H. P. Dai Nguyen and R. Zoltan, "The Current Security Challenges of Vehicle Communication in the Future Transportation System," in Proceedings of the IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), 2018.

[5] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, "Towards Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," in Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP), 2018, pp. 108-116.

[6] A. Halimaa and K. Sundarakantham, "Machine Learning Based Intrusion Detection System," in Proceedings of the 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019.

[7] J. A. Abraham, "Intrusion Detection and Prevention in Networks Using Machine Learning and Deep Learning Approaches," in Proceedings of the International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), 2022.

[8] A. Krishna, A. Lal, A. J. Mathewkutty, D. S. Jacob, and M. Hari, "Intrusion Detection and Prevention System Using Deep Learning," in Proceedings of the International Conference on Electronics and Sustainable Communication Systems (ICESC), 2020.

[9] M. Alazab, P. Poornachandran, R. Vinayakumar, K. P. Soman, A. Al-Nemrat, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, 2019, pp. 52145–52159.

[10] W.-H. Lin, H.-C. Lin, P. Wang, B.-H. Wu, and J.-Y. Tsai, "Using convolutional neural networks for network intrusion detection for cyber threats," in Proceedings of the IEEE International Conference on Applied System Invention (ICASI), 2018, pp. 89-94.

[11] N. Chaabouni, M. Mosbah, A. Zemmari, and C. Sauvignac, "A OneM2M Intrusion Detection and Prevention System based on Edge Machine Learning," in Proceedings of the IEEE/IFIP Network Operations and Management Symposium (NOMS), 2020.