International Journal of Advanced Trends in Engineering and Management
(ISSN 2583-7052)

pp. 14-21, May

An Edge Computing Framework for Real-Time Threat Detection in Autonomous Vehicle Networks

Ashmi P[1], Anugirba K[2]

[1,2] Department of Computer Science and Engineering, Bethlahem Institute of Engineering, Karungal, Kanniyakumari District, Tamil Nadu 629 157, India.

[*] **Corresponding Author**: anurimal21@gmail.com

ABSTRACT: Vehicle Road Cooperation Systems (VRCS) use next-generation Internet technologies, including 5G, edge computing, and artificial intelligence to improve mobility, comfort, and travel efficiency. Autonomous Vehicles (AV) ecosystem serves as the technological backbone for VRCS by enabling seamless communication and data exchange between vehicles, infrastructure, and traffic management centers. This enables real-time, high-speed communication, efficient data processing, and enhanced security, fostering the development of autonomous driving, smart traffic management, and seamless connectivity within the VRCS ecosystem. On the other hand, modeling TI is a challenging task due to the limited labels available for different cyber threat sources. Second, most of the available designs requires a large investment of resources and use hand-crafted features, making the entire process error prone and time-consuming. In order to address these issues, this project suggests TIMIF, a threat intelligence modeling and identification framework for Intelligent AV that is based on deep learning and consists of three main modules: first, the proposed TIMIF adopts an Automated Pattern Extractor (APE) module to extract hidden patterns from AV networks. Employing its output, design a TI-Based Detection (TIBD) module to detect abnormal behavior and TI-Attack Type Identification (TIATI) module to identify attack types. Extensive experiments are carried out on three different publicly intrusion data sources namely ToN-IoT to illustrate the utility of TIMIF framework over some commonly used baselines and state-of-the-art techniques.

Keywords: Autonomous Vehicles, Threat Intelligence, Deep Learning, Cybersecurity, Edge Computing.

1. Introduction

Autonomous vehicle (AV) systems are no longer adequately protected against contemporary cyberthreats by conventional security measures like firewalls and signature-based intrusion detection systems. These methods rely on recognizing known attack patterns, making them largely reactive. As cyberattacks continue to evolve rapidly, these conventional solutions often fail to detect novel or sophisticated attacks, especially those designed to exploit the complex and interconnected nature of AV networks. This creates significant vulnerabilities, as attackers constantly devise new strategies that bypass static defenses.

To overcome these limitations, Threat Intelligence (TI) has emerged as a more proactive and adaptive approach to cybersecurity. TI involves the continuous collection, analysis, and dissemination of data related to existing and emerging threats. Rather than waiting for an attack to occur, TI enables organizations to anticipate risks and prepare defenses in advance. It equips stakeholders with insights into attackers' tactics, techniques, and procedures (TTPs), empowering them to recognize patterns and vulnerabilities before they are exploited. Moreover, collaboration

and information sharing are central to effective TI. Cybersecurity in AV networks is not the responsibility of a single entity; it requires coordinated efforts from multiple stakeholders. Through shared intelligence, organizations can learn from each other's experiences, recognize widespread threats, and collectively build stronger defenses. This collaborative approach not only accelerates response times but also improves the accuracy and relevance of security interventions. In conclusion, Threat Intelligence is indispensable for building resilient cybersecurity frameworks in autonomous vehicle networks. It addresses the shortcomings of traditional defenses by offering predictive capabilities, real-time responsiveness, and collaborative risk management. By embedding TI into the design and operation of AV systems, stakeholders can ensure not only robust protection against cyber threats but also the long-term safety and reliability of smart transportation infrastructures. As autonomous vehicles (AVs) become increasingly sophisticated and connected, they face an expanding range of cybersecurity threats. These threats, ranging from data breaches to real-time attacks on vehicle systems, demand rapid detection and response to ensure vehicle safety and operational integrity. Due to high latency and bandwidth limitations, traditional cloud-based systems frequently find it difficult to meet these requirements. Edge computing helps autonomous car networks meet their real-time cybersecurity needs—which processes data closer to the data's source rather than depending entirely on centralized cloud servers—has shown promise.

- Create a framework for modeling and identifying threat intelligence in the Autonomous Vehicles (AV) ecosystem that is based on deep learning.
- To find hidden patterns in Autonomous Vehicles (AV) networks, implement an Automated Pattern Extractor (APE) module.
- Design a TI-Based Detection (TIBD) module to detect abnormal behaviors within Autonomous Vehicles (AV) systems.
- Create a TI-Attack Type Identification (TIATI) module to accurately identify different attack types.

2. Literature Survey

2.1 A review of vehicle group intelligence in a connected environment

Author: C. Wu, Z. Cai, Y. He, and X. Lu,
Year of publishing: 2024
The research into Vehicle Group Intelligence (VGI) plays a critical role in shaping the future of intelligent transportation systems, aiming to optimize vehicle coordination, enhance safety, and improve traffic flow through collective vehicle behavior. The bibliometric analysis conducted in this study draws on a large dataset of 2821 publications from the SCIE and SSCI databases, offering a detailed overview of the research landscape within VGI. Through a visual analysis from multiple perspectives, the study identifies key trends and knowledge areas that have shaped the development of VGI, such as vehicle platooning, cooperative driving in merging areas, and wireless communication systems for connected vehicles. The research also points out significant gaps and opportunities in the field, such as improving control architectures, addressing application challenges, refining cooperative strategies, and ensuring robust communication protocols and security measures.

2.2 Internet of Vehicles: Architecture, Protocols, and Security

Author: J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibanez
Year of publishing: 2017
The growing adoption of the Internet of Vehicles (IoV) is revolutionizing the way vehicles interact with each other, with infrastructure, and with passengers. As connected vehicles become more ubiquitous, they generate vast amounts of data, necessitating advanced communication systems to enable smooth and continuous data exchange. Traffic efficiency, road safety, and smarter, more autonomous driving are all made possible by the

switch from traditional vehicular ad-hoc networks to autonomous vehicles (AV). These challenges demand innovative solutions and further exploration by the research community to ensure the IoV infrastructure can meet the demands of both current and future transportation systems. Addressing these issues will be crucial for the continued evolution of connected transportation, enabling the realization of fully autonomous and smart cities in the near future.

2.3 A survey on internet of vehicles: Applications, security issues & solutions

Author: S. Sharma and B. Kaushik, "
Year of publishing: 2019
Transportation systems are now highly interconnected and intelligent networks thanks to the Internet of Vehicles (IoV), which expands upon Vehicular Ad-hoc Networks (VANETs) by incorporating the capabilities of the Internet of Things (IoT). The dynamic nature of IoV networks—characterized by rapidly changing topologies, large-scale data exchanges, and real-time communications—poses unique challenges, especially in terms of maintaining security and privacy. IoV systems process sensitive and critical information, such as location data, traffic conditions, and vehicle status, making them prime targets for various cyberattacks, including data breaches, eavesdropping, and malicious interference. As a result, securing IoV networks is a high priority, yet many traditional cryptographic solutions have limitations, especially in delay-sensitive applications like those found in IoV and VANETs. These conventional security mechanisms can introduce significant overhead, impacting network performance and efficiency. This proposed solution aims to balance security and performance, addressing critical vulnerabilities while ensuring the smooth operation of IoV networks.

2.4 Fog based intelligent transportation big data analytics in the internet of vehicles environment: motivations, architecture, challenges, and critical issues

Author: T. S. Darwish and K. A. Bakar,
Year of publishing: 2018
The concept of Intelligent Transportation Systems (ITS) has rapidly evolved with the growth of data-driven applications aimed at improving road safety, traffic management, and environmental sustainability. To address these challenges, the paper proposes a novel architecture that integrates intelligent computing technologies combining cloud and fog computing with the lambda architecture for real-time data processing. This architecture is designed to optimize the processing of IoV data, ensuring faster responses to ITS applications while conserving network resources. The paper also explores the opportunities and potential barriers to implementing fog computing in IoV environments, discussing the necessary technologies and strategies for efficient deployment.

2.5 Intrusion detection model for internet of vehicles using gripca and owelm

Author: K. Zhang, J. Yang, Y. Shao,
Year of publishing: 2024
The rapid expansion of the Autonomous Vehicles (AV) has led to the creation of large-scale, data-intensive networks, where vehicles, infrastructure, and various connected devices generate an enormous amount of data. This data provides valuable insights for traffic management, safety systems, and autonomous driving but also introduces significant security risks. The enormous volumes of data being sent over the network are frequently too much for conventional intrusion detection methods to handle, which causes delays that could seriously affect system security and vehicle safety. In order to address these issues, the suggested model presents a novel strategy that combines optimal weighted extreme learning machine (OWELM) for efficient intrusion detection with Gaussian random incremental principal component analysis (GRIPCA) for dimensionality reduction. These results not only demonstrate the model's superior capability in detecting attacks but also underscore its potential to provide real-time, resource-

efficient solutions for intrusion detection in large-scale AV networks.

2.6 Data Driven intrusion detection for intelligent internet of vehicles: A deep convolutional neural network-based method

Author: L. Nie, Z. Ning, X. Wang,
Year of publishing: 2020
As the operations of Intelligent Transportation Systems (ITS) and the more general idea of smart cities depend more and more on the Internet of Vehicles (IoV), it is critical to make sure that these interconnected systems are secure. The deployment of IoV infrastructure, particularly the Road Side Units (RSUs), creates potential vulnerabilities that can be exploited by malicious actors, leading to disruptions in traffic flow, data breaches, or even more severe attacks on public safety. The Intrusion Detection System (IDS) proposed in this study focuses on monitoring the traffic link loads between RSUs to detect abnormal fluctuations that could signal an attack. Theoretical analysis of this convergence through probabilistic representation ensures that the model is both stable and robust under various operational conditions. The performance of the IDS is thoroughly tested on a dedicated testbed, where it demonstrated high accuracy in identifying attacks, making it a promising solution for real-time security monitoring in IoV networks.

2.7 Mth-ids: A multitiered hybrid intrusion detection system for internet of vehicles

Author: L. Yang, A. Moubayed, and A. Shami,
Year of publishing: 2022
As the integration of electronic control units (ECUs) and vehicle-to-everything (V2X) technologies in modern vehicles continues to enhance their capabilities, it also introduces significant security risks due to the increased complexity and expanded attack surfaces. The safety and functionality of the vehicle may be jeopardized by cyberattacks that target external communication channels and intra vehicle networks (IVNs), which include those that link cars to other cars, infrastructure, and smart devices. This article proposes a multitiered hybrid intrusion detection system (IDS) to address these problems by safeguarding both external and internal vehicular networks. To identify a variety of known and unknown cyberthreats, the suggested intrusion detection system (IDS) combines anomaly-based and signature-based detection methods. By detecting deviations from typical network behavior, the anomaly-based system detects new or zero-day attacks, while the signature-based component identifies known attack patterns. Experiments show that the suggested IDS is effective, with remarkably high accuracy rates of 99.99 % on the CAN-intrusion dataset for IVNs and 99.88 % on the CICIDS2017 dataset for external vehicular network data. Moreover, the system performs well in detecting zero-day attacks, with F1-scores of 0.963 and 0.800 on the respective datasets, indicating its robustness in identifying previously unseen threats. Additionally, the system processes each data packet in under 0.6 milliseconds on a vehicle-level machine, ensuring its suitability for real-time deployment in modern vehicles without compromising system performance.

2.8 Deep learning-enabled threat intelligence scheme in the internet of things networks,

Author: M. Al-Hawawreh, N. Moustafa, S. Garg,
Year of publishing: 2020
With the increasing reliance on Internet of Things (IoT) systems in critical sectors such as Space, Air, Ground, and Sea (SAGS) networks, ensuring the security and safety of these interconnected networks becomes paramount. IoT networks, while enabling automation and improved services, are also vulnerable to a wide range of cyber threats, which can compromise the integrity of the entire system. By detecting cyberthreats and automating incident response, this paper suggests a novel deep learning-based TI scheme to improve SAGS network security. The results demonstrate that the suggested model performs better than current solutions in terms of both detection

accuracy and false alarm rates when tested on two publicly accessible IoT datasets, TON-IoT and N-BAIOT. These findings highlight the effectiveness of the proposed deep learning-based TI scheme in providing a robust and efficient defense mechanism for securing SAGS networks against the growing complexity of cyber-attacks targeting IoT systems.

3. Methodology

The suggested model has been developed and evaluated using the relevant network and threat models. TIMIF framework are discussed briefly in this subsection. 3.1.1 Network Model. The VRCS network is shown in Fig. 3.1 that consist three layers: the physical layer, virtual layer, and management layer. This layer is crucial for TIMIF, particularly for the TI-Based Detection (TIBD) module, which utilizes the processed data to detect abnormal behaviors indicative of cyber threats. The assumption here is the layer's ability to maintain end-to-end elasticity, ensuring that the TIMIF framework can scale according to the volume of data and complexity of threats encountered. Throughout the network model, we assume that communication occurs over potentially insecure channels, a reality that underscores the importance of TIMIF's role in the AV ecosystem. This assumption drives the necessity for robust threat detection and identification mechanisms capable of operating effectively despite the inherent vulnerabilities of these communication pathways

3.1 Existing System

The existing systems for cybersecurity in autonomous vehicle (AV) networks often rely on traditional machine learning techniques, with Decision Trees (DT) being one of the most commonly used methods. In these systems, Decision Trees are utilized for tasks such as intrusion detection, anomaly detection, and sensor data validation. Although decision trees can perform fundamental security tasks, they are becoming less and less effective in the face of increasingly complex and quickly changing cyberthreats, underscoring the need for more sophisticated, adaptable systems.

3.2 Proposed System

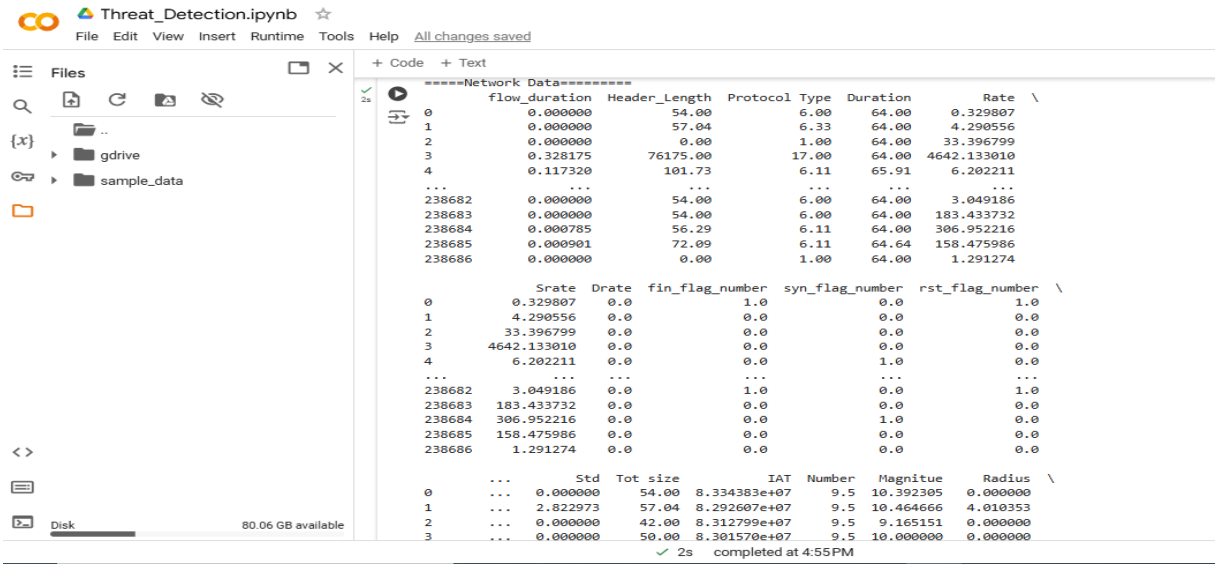
The proposed system, TIMIF (Threat Intelligence Modeling and Identification Framework), is designed to enhance cybersecurity for Autonomous Vehicle (AV) networks by automating the detection and identification of cyber threats using advanced deep learning (DL) techniques. TIMIF addresses the limitations of existing systems by incorporating a three-tier architecture that leverages the physical, virtual, and management layers of a Vehicle Roadside Communication System (VRCS). At the physical layer, data is generated by intelligent vehicles and IoT devices, including onboard units (OBUs) that capture environmental conditions, driving patterns, and critical events. This data serves as the primary input for the system, which is processed initially by the Automated Pattern Extractor (APE) module. Finally, the Threat Intelligence-Attack Type Identification (TIATI) module classifies the detected threats into specific attack types. This module utilizes an Extended Self-Attention-based Deep Bidirectional Gated Recurrent Unit (ESA-DBGRU) algorithm to assign appropriate weights to relevant data sequences and improve the precision of threat classification. Extensive testing on publicly available datasets verifies the framework's superior performance over both conventional and cutting-edge approaches.

3.3 Modules Description

In order to prepare raw data for efficient analysis within the TIMIF framework, the data preprocessing stage is essential. Initially, raw input data collected from the autonomous vehicle (AV) network is cleaned to handle missing values, normalize numerical features, and address any inconsistencies that could impact the accuracy of the threat detection process. The preprocessing involves several key steps: **normalization**, where a min-max normalization technique is applied to

scale the numerical values of features within a defined range (typically [0,1]), ensuring that features with different scales do not disproportionately influence the model. **Missing value imputation** is also performed, where any incomplete or missing data points are filled using the column mean or median, preserving data integrity and preventing data loss. Next, **feature encoding** is applied to categorical variables, converting them into numerical formats using techniques such as label encoding or one-hot encoding to make the data compatible with machine learning algorithms. Finally, the dataset is split into a **training set** (typically 70%) and a **testing set** (30%), where the training set is used for model building and the testing set is reserved for model evaluation.

4. Results and Discussion



4.1 Discussion

In this project, compared the performance of a Decision Tree (DT) classifier with a proposed method across four key evaluation metrics**:** accuracy**,** precision**,** recall, and F1 score. Based on the results, the proposed method clearly outperforms the Decision Tree in all evaluated areas, which suggests that it provides a more effective solution for the classification task at hand.

Table 1: Performance Metrics

Methods	Accuracy	Precision	Recall	F1score
Decision Tree(DT)	92.20	90.11	89.21	88.12
Proposed	0.9467	0.9464	0.9467	0.9455

True Positives (TP), False Positives (FP), False Negatives (FN), and True Negatives (TN) are the four categories into which the confusion matrix divides a classifier's predictions to give a comprehensive picture of how well it is performing. Additional performance metrics like accuracy, precision, recall, and F1 score can be computed using these four values. Understanding the advantages and disadvantages of each mode is possible through a closer look at the confusion matrix for the suggested approach.

5. Conclusion and Future Work

The TIMIF framework, in summary, provides a thorough and efficient method for detecting cyber threats in autonomous car networks in real time. The modular design, which includes the Automated Pattern Extractor (APE), Threat Intelligence-Based Detection (TIBD), and Attack Type Identification (TIATI) components, ensures that the framework can detect and classify a wide range of cyber-attacks, improving both the accuracy and scalability of threat detection.

Moreover, the use of edge computing in TIMIF addresses key challenges related to low-latency data processing and high-volume traffic, crucial for autonomous vehicle environments. By performing data analysis locally at the edge, TIMIF reduces communication delays and enhances the system's ability to detect threats in real-time, providing a timely response to potential security incidents. Tested on publicly accessible datasets, the framework's performance surpasses both conventional approaches and the most advanced techniques currently in use in terms of detection efficiency and accuracy.

References

1. Chaozhong Wu; Zhenggan Cai; Yi He; Xiaoyun Lu, Sherali Zeadally, and Juan Antonio Guerrero-Ibañez, Year: 2024, “A review of vehicle group intelligence in a connected environment,” IEEE Transactions on Intelligent Vehicles, Vol: 9, No: 1, pp. 1865–1889.
2. Juan Contreras-Castillo; Sherali Zeadally; Juan Antonio Guerrero-Ibañez, Year: 2017, “Internet of vehicles: architecture, protocols, and security,” IEEE internet of things Journal, Vol: 5, No: 5, pp. 3701–3709.
3. Surbhi Sharma; Baijnath Kaushik, Year: 2019 “A survey on internet of vehicles: Applications, security issues & solutions,” Vehicular Communications, Vol: 20, pp. 100182.
4. Tasneem SJ Darwish; Kamalrulnizam Abu Bakar, Year: 2018, “Fog based intelligent transportation big data analytics in the internet of vehicles environment: motivations, architecture, challenges, and critical issues,” IEEE Access, Vol: 6, pp. 15 679–15 701.
5. Kaijun Zhang; Jiayu Yang; Yangfei Shao; Lehua Hu; Wei Ou; Wenbao Han; Qionglu Zhang, Year: 2024, “Intrusion detection model for internet of vehicles using gripca and owelm,” IEEE Access, 2024.
6. Achref Haddaji; Samiha Ayed; Lamia Chaari Fourati, Year: 2024, “A novel and efficient framework for in-vehicle security enforcement,” Ad Hoc Networks, pp. 103481.
7. Laisen Nie; Zhaolong Ning; Xiaojie Wang; Xiping Hu; Jun Cheng; Yongkang Li, Year: 2020, “Datadriven intrusion detection for intelligent internet of vehicles: A deep convolutional neural network-based method,” IEEE Transactions on Network Science and Engineering, Vol: 7, No: 4, pp. 2219–2230.
8. Li Yang; Abdallah Moubayed; Abdallah Shami, Year: 2022, “Mth-ids: A multitiered hybrid intrusion detection system for internet of vehicles,” IEEE Internet of Things Journal, Vol: 9, No: 1, pp. 616–632.
9. Brooke Lampe; Weizhi Meng, Year: 2023, “Intrusion detection in the automotive domain: A comprehensive review,” IEEE Communications Surveys Tutorials, Vol: 25, No: 4, pp. 2356–2426.
10. Muna Al-Hawawreh; Nour Moustafa; Sahil Garg; M. Shamim Hossain, Year: 2020, “Deep learning-enabled threat intelligence scheme in the internet of things networks”, IEEE Transactions on Network Science and Engineering, pp. 1–1.
11. Paris Koloveas; Thanasis Chantzios; Sofia Alevizopoulou; Spiros Skiadopoulos; Christos Tryfonopoulos, Year: 2021 “intime: A machine learning-based framework for gathering and leveraging web data to cyber-threat intelligence”, Electronics, Vol: 10, No: 7, pp. 818.
12. Masashi Kadoguchi; Shota Hayashi; Masaki Hashimoto; Akira Otsuka, Year: 2019, “Exploring the dark web for cyber threat intelligence using machine leaning,” in 2019 IEEE International

Conference on Intelligence and Security Informatics (ISI). IEEE, 2019, pp. 200–202.

13. Danny Dolev; Andrew Yao, Year: 1983, "On the security of public key protocols," IEEE Transactions on information theory, Vol: 29, No: 2, pp. 198–208.
14. Alsaedi Abdullah; Nour Moustafa; Zahir Tari; Abdun Mahmood; Adnan Anwar, Year: 2020, "Ton iot telemetry dataset: a new generation dataset of iot and iiot for data-driven intrusion detection systems," IEEE Access, Vol: 8, pp. 165 130–165 150.
15. Nour Moustafa; Erwin Adi; Benjamin Turnbull; Jiankun Hu, Year: 2018, "A new threat intelligence scheme for safeguarding industry 4.0 systems," IEEE Access, Vol: 6, pp. 32 910–32 924.
16. Venkata Atluri; Jeff Horne, Year: 2021, "A machine learning based threat intelligence framework for industrial control system network traffic indicators of compromise," in SoutheastCon 2021. IEEE, 2021, pp. 1–5.
17. Nighat Usman; Saeeda Usman; Fazlullah Khan; Mian Ahmad Jan; Ahthasham Sajid; Mamoun Alazab; Paul Watters, Year: 2021, "Intelligent dynamic malware detection using machine learning in ip reputation for forensics data analytics," Future Generation Computer Systems, Vol: 118, pp. 124–141.
18. Umara Noor; Zahid Anwar; Asad Waqar Malik; Sharifullah Khan; Shahzad Saleem, Year: 2019 "A machine learning framework for investigating data breaches based on semantic analysis of adversary's attack patterns in threat intelligence repositories," Future Generation Computer Systems, Vol: 95, pp. 467–487.
19. H. K. KIM, Year: 2018, "Car hacking dataset," online; accessed 1- Feb-2024. [Online]. Available: https://ocslab.hksecurity.net/Datasets/ CAN-intrusion-dataset
20. N. Moustafa, Year: 2019, "Ton iot datasets," online; accessed 2020.
21. I. Sharafaldin, Year: 2017, "Cic-ids2017 datasets", online; accessed 15-Mar-2019. [Online]. Available: http://205.174.165.80/CICDataset/ CIC-IDS-2017/Dataset/
22. Wei Lo; Hamed Alqahtani; Kutub Thakur; Ahmad Almadhor; Subhash Chander; Gulshan Kumar, Year: 2022, "A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic," Vehicular Communications, Vol: 35, pp. 100471.
23. Izhar Ahmed Khan; Nour Moustafa; Dechang Pi; Waqas Haider; Bentian Li; Alireza Jolfaei, Year: 2022, "An enhanced multi-stage deep learning framework for detecting malicious activities from autonomous vehicles," IEEE Transactions on Intelligent Transportation Systems, Vol: 23, No: 12, pp. 25 469–25 478.
24. Yanqing Yang; Kangfeng Zheng; Bin Wu; Yixian Yang; Xiujuan Wang, Year: 2020 "Network intrusion detection based on supervised adversarial variational auto-encoder with regularization," IEEE Access, Vol: 8, pp. 42 169–42 184.
25. S. Priya and R. Annie Uthra, Year: 2021, "An effective deep learning-based variational autoencoder for zero-day attack detection model," in Inventive Systems and Control. Springer, 2021, pp. 205–212.
26. Mengxuan Tan; Alfonso Iacovazzi; Ngai-Man Man Cheung; Yuval Elovici, Year: 2019, "A neural attention model for real-time network intrusion detection," in 2019 IEEE 44th Conference on Local Computer Networks (LCN). IEEE, 2019, pp. 291–299.