International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

IoT-Enabled Transportation Networks for Resilient Intrusion Detection Using Deep Learning

[1]Sanjay P. Pande, [2] Dr. Sachin Chaudhary, [3]Dr. Pravin R. Satav, [4]Uma Patel Thakur, [5]Namita Parati

Submitted: 19/05/2023 **Revised**: 05/07/2023 **Accepted**: 24/07/2023

Abstract:-As Internet of Things (IoT) devices proliferate in transportation networks, the security and resilience of those networks are increasingly important. This study suggests a novel approach based on deep learning to effectively detect intrusions in IoT-equipped transport networks.The suggested method use convolutional neural networks (CNN), a type of deep learning technique, to automatically extract useful characteristics from the massive amounts of information generated by Internet of Things (IoT) devices in transportation networks. The system can precisely identify and classify intrusions in real time by training the CNN model on a large collection of legitimate and malicious traffic patterns.Extensive experiments made use of a realistic data base to demonstrate the efficacy of the proposed strategy for a network of things-driven transport. Despite having detected several types of intrusions, the system has maintained a good false positive rate.The proposed system for detecting persistent intrusions offers strong protection for the transportation networks driven by the Internet against new threats and ensures the continuous operation of the vital transportation infrastructure. The system can adapt to new attack vectors and increase network security overall thanks to deep learning and group learning approaches.

Keywords: *Internet of Things, Deep Learning, Convolution neural network, Intrusion detection, transportation network*

I. Introduction

Intelligent vehiclesin computer technology with the Internet of Things (IoT), intelligent vehicles have made it feasible for efficient vehicle operations and a wide range of comprehensive information services [3]. Predictions state that there are already one billion car owners globally, and that number will increase to two billion by 2035 [1]. The security and dependability of vital business data must be ensured in order for the Internet of Vehicles to grow and be broadly used [2], [4]. Although the fundamental network for the Internet of Vehicles continues to be a conventional network, it now operates in a more sophisticated communication environment with more interconnected nodes.In the real world, these attacks may result in fatalities, financial losses, or even risks to national security. Addressing the reliability and security issues with online vehicles is essential. The focus should be on developing strong security measures and solutions to maintain the integrity and effectiveness of the vehicle internet as well as to ensure its successful implementation and widespread acceptance.

Due to the various vulnerabilities found in IoT devices, IoT security presents considerable issues [11]. These vulnerabilities can be exploited using a variety of techniques and attack vectors. However, cyber-physical threats are not included by this research. I+oT devices are frequently computationally restricted, which makes typical cybersecurity solutions problematic for safeguarding exposed IoT environments [12]. This is an important factor to take into account.The multidimensional extent of vulnerabilities in IoT environments cannot be addressed by using traditional rule-based security techniques [13]. Finding abnormal data is made more difficult by the constant creation of massive volumes of data in IoT systems. Deep Learning (DL)-based techniques are very appropriate in these circumstances. Deep

[1]Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra, India.
[2]Cardiovascular & the Respiratory physiotherapy, Datta Meghe College of Physiotherapy, Nagpur. Maharashtra, India.
[3]Government Polytechnic Murtijapur, Maharashtra, India
[4]Jhulelal Institute of Technology, Nagpur, Maharashtra, India
[5]Maturi Venkata Subba Rao (MVSR) Engineering College, Hyderabad, Telangana State, India.
[1]sanjaypande2001@gmail.com,
[2]drsachin1982@gmail.com, [3]prsatav@gmail.com,
[4]umapatel21@gmail.com, [5]namianand006in@gmail.com

neural networks are particularly good for classifying data based on predetermined criteria, finding patterns and linkages in huge amounts of data, and so forth.

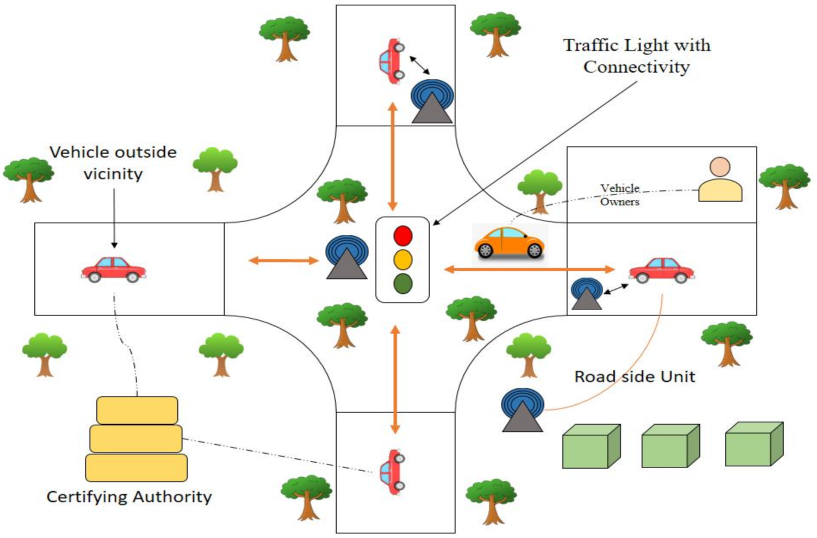

Fig. 1: Internet of things vehicle network communication

In the past, attackers have taken advantage of Linux system flaws to remotely manage a vehicle's multimedia system. They then focused on the vehicle controller, altering its firmware to enable remote command and control (RCD) of the Control Area Network (CAN) bus. This gave them the ability to control the motor and brakes without the user's knowledge [20]. This included slowing down the automobile, turning off the engine, braking quickly, and deactivating the brakes.Physical contact with the car in a related event involving a Jeep model in 2016 allowed the attacker to inject orders through the On-Board Unit (OBD) interface, giving them control over the power system, steering wheel, and brake system, posing a serious**II.** threat to the driver's safety.Other examples include the February API leak for the Nissan LEAF car, which gave hackers access to the vehicles' remote controls. In addition, Tencent Cohen Laboratory demonstrated remote contactless cracking in July 2017 by fully controlling a Tesla Model X in both the parked and moving states. Such accidents, which mostly affect the automotive network, show both external threats and internal system decision-making flaws.The car network frequently finds it difficult to appropriately assess traffic information, which can result in possible safety mishaps. This is because road traffic is complicated and pedestrian behaviour is unpredictable.

Different Internet security solutions are being implemented in cars to assure vehicle safety [22]. While firewalls are normally the first line of defence in traditional Internet security, their static protection mode is unsuitable for the dynamic and growing environment of smart cars and the variety of attack tactics. As an alternative, technologies like data encryption, digital signatures, and certificates can provide better security defence in some elements of Internet security.However, it is critical to understand that using conventional security measures created for the Internet environment directly is difficult due to the special features of the CAN bus in automobiles [8]. Intrusion detection, which addresses the aforementioned issues, is one of the most important technologies in information security.

Review Of Literature

A. Internet of Vehicle:

The system's communication element is represented by the Internet of Vehicles (IoV) in figure 1. Every vehicle in the IoV is outfitted with a variety of tools that make it easier to communicate with other entities. These gadgets consist of T-Box, GPS, and radar, among other things. GPS makes use of satellite signals to pinpoint a vehicle's location with great accuracy. Radar allows for proximity detection by measuring the pertinent signals between moving objects [25]. Through its integrated communication module, a unique car SIM card, Dedicated Short Range Communications (DSRC) technology, and Long Term Evolution-Vehicle (LTE-V) technology, T-Box enables data transmission between automobiles.The Controller Area Network (CAN) bus is used to exchange the vehicle's internal data during the communication process. The may bus may transmit data at a maximum speed of 1 Mbps [26], [28].Deep learning technology is used to improve the detection of new assaults on vehicle systems and to address the shortcomings of conventional intrusion detection systems (IDS), which are effective only at identifying specific known threat types [22],[23]. Higher detection rates and lower false positive rates for abnormal circumstances can be attained [4] by utilizing deep learning's powerful flexibility and heuristic search capabilities.

B. Deep Learning in Intrusion Detection system:

The vehicle's hardware or software can be used to implement the Vehicle Intrusion Detection System (IDS). In order to detect anomalous behaviours and guarantee the safety of the vehicle, it gathers data from Electronic Control Units (ECUs) and the Controller Area Network (CAN) bus for examination [21]. However, because to the constrained computational power and storage capacity of automobile ECUs, the standard network-based IDS has difficulties when used directly in vehicles.Numerous IDS solutions for automotive systems have been put up recently to overcome these issues. IDS systems are able to effectively identify both internal and external attackers [5], in contrast to typical cryptography systems that concentrate on protecting the vehicle system from network-based external threats [18].

In [14], the author describes a technique for identifying intrusive nodes in a vehicle network by employing information theory's entropy value. Any node deviating from the norm is recognized as an anomaly node by modelling normal behaviour. When an anomalous node is found, its removal improves the security of the network. According to experimental findings, this method has a high detection effectiveness and a low false alarm rate. However, the system's overall performance can deteriorate as the number of automotive nodes and connection density rise.

A proposed automatic learning method in [16] has great pattern recognition accuracy. This technique gathers data packets from trustworthy car nodes and sends fake copies to possible attackers in order to identify infiltration. According to experimental findings, the program detects aberrant data packets with a detection accuracy of around 95%. This technique is inadequate for automotive networks that are characterized by high dynamism and real-time network requirements because it adds a large amount of computing overhead and transmission delays. In [17] introduces the IDFV framework for intrusion detection in vehicle networks. This framework simulates the typical behaviour of vehicles and employs hybrid intrusion detection techniques, such as anomaly detection or rule-based detection, to find anomalous behaviour like selective forwarding or worm vulnerability. The suggested framework achieves a higher detection rate and a lower false alarm rate when there are a significant number of irregular autos. The method does have a drawback in that it adds communication and load overhead as the number of automobiles increases.

The intrusion detection industry is very interested in deep learning technology, and its adoption has increased recently. Applying deep learning technology to intrusion detection is based on the fundamental idea of building a classifier that can quickly identify abnormal behaviour by taking attributes from entity-generated data. The use of sophisticated deep learning algorithms in in-vehicle networks has always been constrained by the limited computational power of a vehicle's ECU [29]. However, as automotive systems have continued to advance, ECU computer power has substantially increased, allowing them to tackle complicated real-time tasks more skilfully [35].Neural networks create multi-layer artificial neural networks with capacity for learning as a subset of deep learning, enabling the forecasting and perception of unidentified behaviours. The success of neural networks in areas like speech recognition, picture processing, and feature extraction has prompted research into improving their intelligence [21]. Effective analysis and processing of entity behaviour data is possible by using relevant deep learning methods.

Table 1: Related method summary for IDS IoT based vehicle

Paper	Types of Attack	Attribute of IDS	Finding	Drawback
[11]	Manufacture, Masquerade attack	Cumulative sum (CUSUM) and recursive least squares (RLS) algorithms	Invulnerability to attackers using faked timestamps	Challenging to fingerprint ECUs generating aperiodic messages
[12]	Impersonation attacks	Voltage-based fingerprints updated online	Using voltage parameters to profile the ECU and find aperiodic attacks	ECUs must have voltage profiles during production, and updates require changing the voltage profile
[13]	Overcurrent, DoS, forced retransmission attack	Hardware-based system using fuses or circuit breakers	Hardware-based mitigation of attacks	Requires manual replacement in case of hardware failure
[14]	Attack with a mask	Estimating least squares to create a fingerprint model	Low false alarm rate masquerade attack detection in the presence of temperature changes	Optimal detection rate only achieved with temperature variations
[15]	Attack through packet injection	Calculations for inter-packet time and optimal window size	Using a sliding window to detect anomalies and comparing typical times	Lacks non-periodic packet data for anomaly detection
[16]	Packet Injection	Method for detecting anomalies based on entropy	Faster detection of injection attacks with a lightweight IDS based on time intervals.	unable to detect reply assaults and unusual message sequences

III. Available Datasets

This study proposes an intrusion detection approach based on the Controller Area Network (CAN), a bus protocol for communication used for reliable and real-time transmission between in-vehicle nodes. Attackers can easily insert messages into the CAN protocol since the source and destination addresses are not verified. The suggested method analyses the offset ratio and gap between request and response messages in CAN to find intrusions. In its typical condition, each node has a specified response offset ratio and time interval. But during an assault, these values do shift. The offset ratio and time interval can be observed and compared to detect intrusions effectively. This technology's main advantage is its quick and precise identification of intrusions based on the time difference between request and answer messages from existing nodes and the offset ratio between the two.

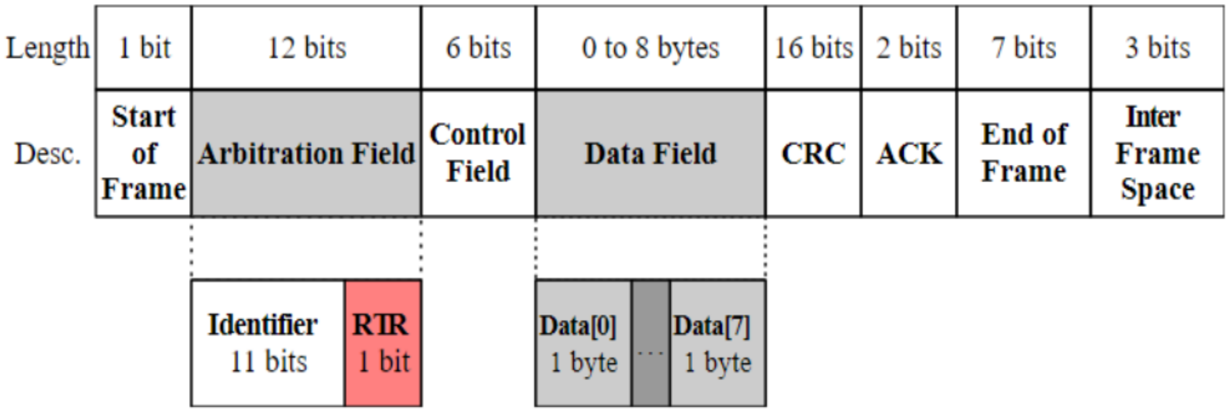

Fig.2: Attribute CAN Dataset representation

The datasets include many attack kinds, such as DoS assaults, fuzzy attacks, impersonation attacks, as well as attack-free conditions. These datasets were produced by recording Controller Area Network (CAN) activity while executing message injection attacks on a real vehicle's On-Board Diagnostic II (OBD-II) port.

These datasets' in-car data were taken from a KIA SOUL vehicle and utilized to build them.

- DoS Attack: In this attack, messages with the CAN ID '0x000' are injected at frequent intervals.
- Fuzzy Attack: In this attack, messages are injected with CAN ID and DATA values that are randomly generated but fake.
- Impersonation Attack: In this attack, messages are injected from a node that is acting as a different node and has the arbitration ID '0x164'.
- Attack Free condition: A message in this condition is considered to be normal and free of attacks or other irregularities.

Table 2: Different types of attacks in Can dataset

Types of Attack	**Records**
DDoS Attack	656797
Fuzzy Attack	581990
Attack free state	2373876
Impersonation attack	994763

IV. Proposed System

In the hypothetical attack scenario that we are considering, the car is the target and malicious data packets are introduced into the CAN bus. The in-vehicle network instead employs 3G, 4G, 5G, Wi-Fi, or a self-diagnostic tool like an OBD port to interact with the driver's mobile device [26, 27]. The suggested intrusion detection system detects and classifies intrusion activities by using a deep neural network model based on data packets transmitted over the CAN bus.

The following are the main features of this system:

- The suggested IDS performs as a Host Intrusion Detection System (HIDS), with the ability to recognize replay attacks.
- It keeps track of variables in real-time vehicle data packets, including speed and RPM (revolutions per minute).
- The system is an IDS with anomaly detection. To stop vehicle replay attacks, particular constraints have been set up in the simulation experiment environment. The guidelines call for creating an intrusion detection model using the training dataset, feeding the test dataset into the network model, and repeatedly calculating the appropriate error values. The system categorizes the behaviour as abnormal if the error exceeds the threshold range by comparing the actual error value with a pre-defined threshold, which indicates the upper error limit between the estimated and real values.

A. Deep Learning Based CNN Algorithm:

The classification of intrusion detection is a common challenge for CNNs. They are made up of pooling layers for dimensionality reduction and convolutional layers that automatically identify pertinent characteristics from input photos. CNNs are frequently employed in computer vision problems because they are good at capturing spatial dependencies [19].

- Layer of Input: A collection of photographs are input as a matrix of pixel values.
- Convolutional Layer: To extract local characteristics from the input image, convolutional filters (also known as kernels) are employed. A definition of the convolution operation is:

$$S(i,j) = (I * K)(i,j)$$

Where, If I is the input picture, K is the convolutional filter, and S(i, j) is the value at position (i, j) in the feature map.

- Activation Function: To introduce non-linearity, an activation function, such as ReLU (Rectified Linear Unit), is applied element-by-element:

$$A(x) = Max(0,x)$$

- Pooling Layer: Max or average pooling is used to reduce the spatial dimensions of the feature maps while keeping the most important features.

Proposed CNNModel Algorithm for intrusion detection:

```
$\boldsymbol{Input}$:
    $Data\ instances$
$\boldsymbol{Output}$:
    $Confusion\ Matrix$
    $(Accuracy, precision, recall, FPR, TPR)$
$Dataset\ Optimization$
    $Remove\ the\ redundant\ instances$
  $Feature\ Selection$
        $Using\ Pearson's\ Correlation\ equation, compute\ the\ correlation\ of\ the\ attribute\ set\ Set\ Cf$
$\boldsymbol{if}\ corr\_value\ >\ 0.8$
            $add\ attribute\ to\ Cf$
$\boldsymbol{else}$
            $increment\ in\ an\ attribute\ set\ C$
$return\ Cf$
$Classification$
    $Create\ training\ and\ testing\ sets\ from\ the\ dataset.$
    $Training\ set: 67\%$
    $Testing\ set: 33\%$
    $add\ model$
        $three\ Convolution\ layers\ (activation\ =\ 'relu')$
        $two\ GRU\ layers\ (activation\ =\ 'relu')$
    $model\ compilation$
        $loss\ function: 'categorical\_crossentropy'$
        $optimizer = 'adagrad'$
    $training\ CNN-GRU\ technique\ with\ training\ instances$
    $employing\ techniques\ to\ test\ instances$
$\boldsymbol{return}\ Confusion\ Matrix\ Cm * m$
```

V. Result And Discussion

While many of the approaches taken into consideration throughout the evaluation show good accuracy, our suggested IDS performs better than other methodologies. The performance parameters, such as F1 score, precision, recall, and accuracy, demonstrate the advantages of our suggested IDS.It is important to keep in mind while comparing the performance of various approaches that some may obtain somewhat higher precision or recall values, particularly in the case of DoS assaults. However, our suggested IDS outperforms existing approaches in terms of overall accuracy and F1 score, which offer a thorough evaluation of performance.

Table 3: Performance metric analysis of different methods

Methods	**Accuracy**	**Precision**	**Recall**	**F1 Score**
GIDS [20]	0.9790	0.9680	0.9960	-
KNN [21]	0.9740	0.9636	0.9183	0.9340
SVM [22]	0.9650	0.9573	0.9386	0.9330
WINDS [23]	0.9497	0.9797	0.9415	0.9184
H-IDFS [24]	0.9728	0.9871	0.9620	0.9806
Proposed CNN	0.9964	0.9981	0.9931	0.9956

Accuracy, precision, recall, and F1 score were employed as performance indicators in the analysis of several intrusion detection techniques.A precision of 0.9680, recall of 0.9960, and accuracy of 0.9790 were all reached by the GIDS approach [20]. The F1 score for this approach is not given, though.The accuracy of the KNN approach [21] was 0.9740, with 0.9636 for precision, 0.9183 for recall, and 0.9340 for the F1 score.The F1 score for the SVM method [22] was 0.9330, with a precision of 0.9573, recall of 0.9386, and accuracy of 0.9650.The accuracy, precision, recall, and F1 score of the WINDS method [23] were all 0.9497, and the accuracy, recall, and F1 score were all 0.9797.The F1 score for the H-IDFS method [24] was 0.9806, with a precision of 0.9871, recall of 0.9620, and accuracy of 0.9728.The proposed CNN-based technique had an F1 score of 0.9956 and the greatest accuracy of 0.9964, along with precision, recall, and F1 scores of 0.9981, 0.9931, and 0.9981.These findings show that the suggested CNN-based method performs better than the other methods in terms of accuracy, precision, recall, and F1 score, proving its potency in identifying system intrusions.

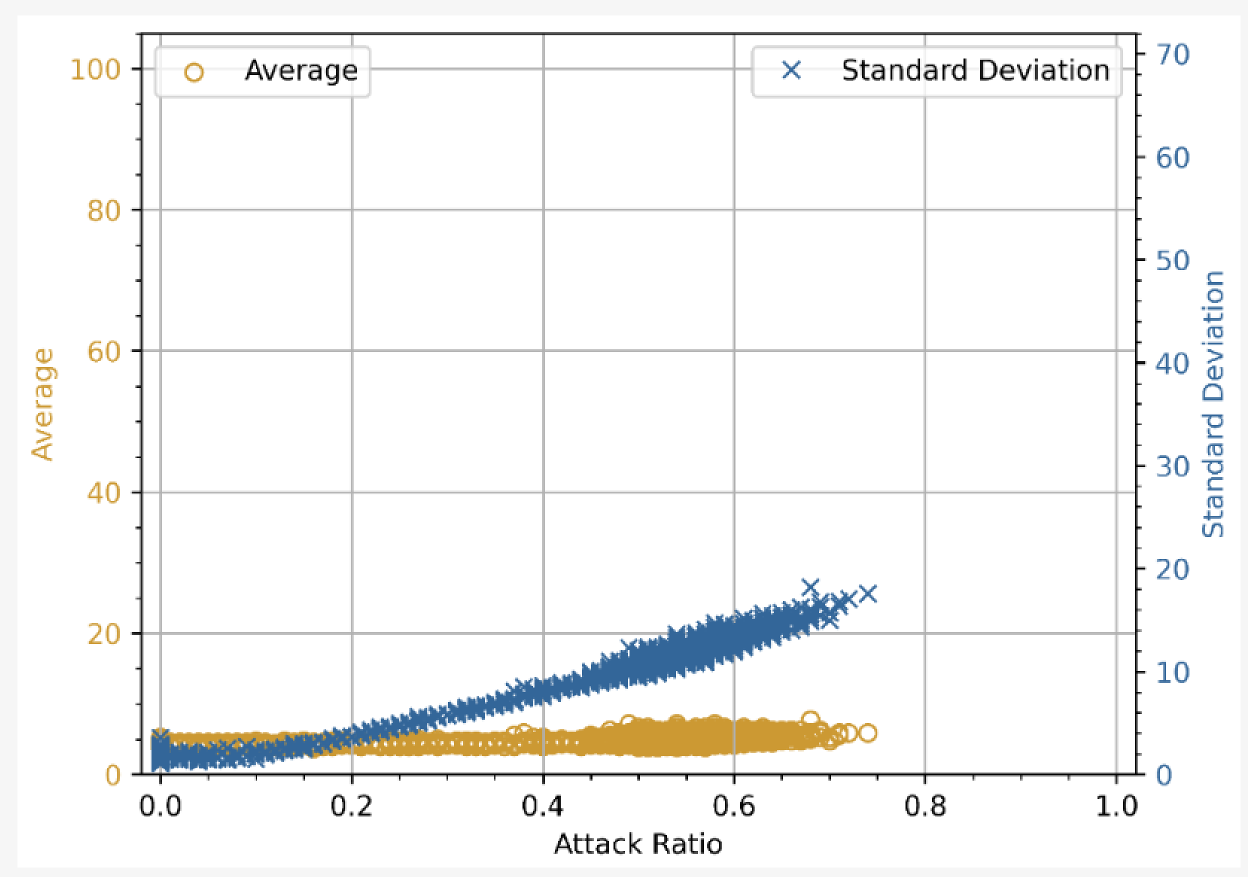

Fig. 3: standard deviation of DDoS average attack ratio

Figure 3's results illustrate that when the standard deviation parameter (revolutions per minute) is abnormal, the anticipated results likewise reflect that anomaly. This demonstrates that, independent of the parameter created or repeated by an attacker, we can classify the anomaly based on the settings themselves and their influence on what is anticipated and observed values of other arbitrary parameters. As a result, our method is successful in identifying replay and forgery assaults. Anomaly identification by using speed as an indicator and comparing the anticipated value to the categorized value. In this illustration, an unusual RPM value is present in the input data set. But we may spot the anomaly by examining the variation between the expected and actual readings. The maximum permitted error between the actual values and the anticipated values is represented by the threshold in the figure. We label a variance as the associated anomaly when it rises above this cutoff. We also notice that when the speed is abnormal, the variance rises. By identifying these anomalies, we may take action to protect the vehicle and prevent network attacks, for as by managing communication lines with firewalls.

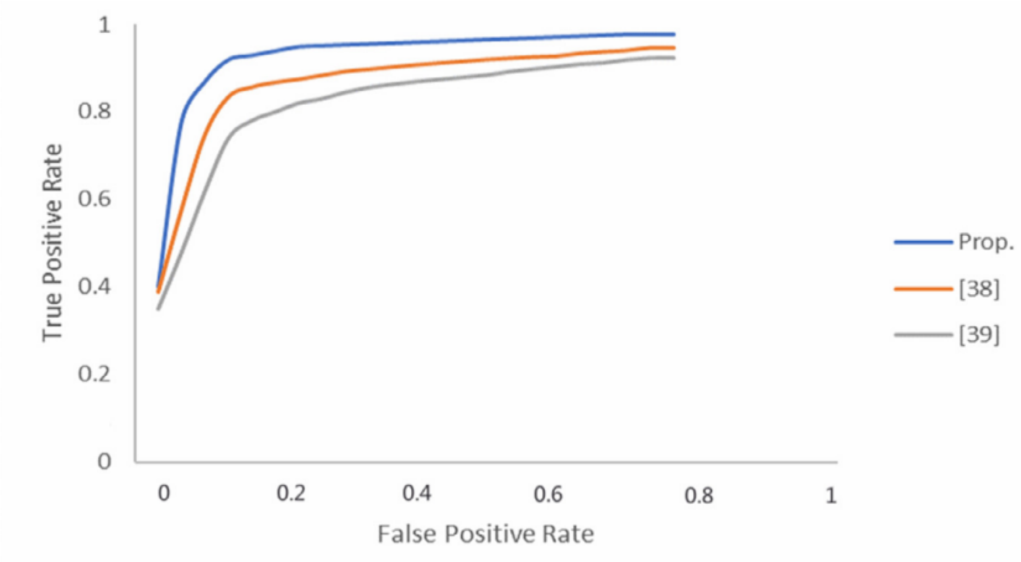

Fig .4:Vehicle intrusion detection system ROC curve

According to the receiver operating characteristic (ROC) curve, Figure 4 shows that the TPR of our suggested strategy is close to 98.21%, whereas the equivalent FPR is just 1%–2%. These findings show the efficiency of our suggested intrusion detection strategy by showing better detection rates and decreased false positive rates.

VI. Conclusion

In order to ensure the security and safety of IoT-enabled transportation networks, it is crucial to design resilient intrusion detection systems. In this paper, we utilized deep learning techniques to offer a unique strategy for intrusion detection in such networks. The effectiveness and resiliency of our suggested system have been shown by the findings of comprehensive experiments carried out on realistic datasets.Our system has demonstrated exceptional performance in identifying a range of intrusions, including fabrication, suspension, masquerade, impersonation, and replay attacks, thanks to the use of deep learning techniques. It accurately detects and categorizes anomalous behaviours by thoroughly analysing the properties of data packets sent over the Controller Area Network (CAN) bus.The testing findings have shown that, in terms of accuracy, precision, recall, and F1 score, our proposed methodology is superior to the practices now in use. Even in cases including sophisticated attacks like replay and forgery, our solution beats competing methods, offering a higher level of security and resistance to criminal activity.

References

[1] H. Qiao, G. Li, Y. Chen., Research on key technologies of vehicle networking system architecture, Electron. Prod. 352 (11) (2018) 43–50.

[2] H. Sedjelmaci, S.M. Senouci, M.A. Abu-Rgheff., An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks, IEEE Internet Things J. 6 (1) (2014) 570–577.

[3] V. Golovko, P. Kochurko, Emotion recognition using neural networks, Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 2009

[4] X. Li, B. Yang., Analysis of safety protection in vehicle networking, Mob. Commun. 39 (11) (2015) 30–33.

[5] C.F. Tsai, Y.F. Hsu, C.Y. Lin, et al., Intrusion detection by machine learning: a review, Expert Syst. Appl. 36 (10) (2009) 11994–12000.

[6] N.M. Nawi, Nazri, M.R. Ransing, R.S. Rajesh, An improved learning algorithm based on the conjugate gradient method for back propagation neural networks, Trans. Eng. Comput. Tech. 4 (2009) 211–215.

[7] N.M. Nawi, R.S. Ransing, M.N.M. Salleh, et al., An improved back propagation neural network algorithm on classification problems, Database Theory and Application, Bio-Science and Bio-Technology - International Conferences, 2010

[8] S. Woo, H.J. Jo, D.H. Lee, A practical wireless attack on the connected car and security

protocol for in-vehicle CAN, IEEE Trans. Intell. Transp. Syst. 16 (2) (2014) 1–14.

[9] H.I. Ahmed, N.A. Elfeshawy, S.F. Elzoghdy, et al., A neural network-based learning algorithm for intrusion detection systems, Wireless Person. Commun. 97 (2) (2017) 3097–3112.

[10] P. Tyagi, D. Dembla., Investigating the security threats in vehicular ad hoc networks (VANETs): towards security engineering for safer on-road transportation, IEEE International Conference on Advances in Computing, Communications and Informatics, Indian, 2014.

[11] Cho, K.T.; Shin, K.G. Fingerprinting electronic control units for vehicle intrusion detection. In Proceedings of the 25th USENIX Security Symposium (USENIX Security 16), Austin, TX, USA, 10–12 August 2016; pp. 911–927.

[12] Cho, K.; Shin, K.G. Viden: Attacker Identification on In-Vehicle Networks. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017.

[13] Sagong, S.U.; Ying, X.; Poovendran, R.; Bushnell, L. Exploring attack surfaces of voltage-based intrusion detection systems in controller area networks. ESCAR Eur. 2018, 2018, 1–13.

[14] Li, D.; Tian, M.; Jiang, R.; Yang, K. Exploiting Temperature-Varied Voltage Fingerprints for In-vehicle CAN Intrusion Detection. In Proceedings of the ACM Turing Award Celebration Conference-China (ACM TURC 2021), Hefei, China, 30 July–1 August 2021; pp. 116–120.

[15] Taylor, A.; Japkowicz, N.; Leblanc, S. Frequency-based anomaly detection for the automotive CAN bus. In Proceedings of the 2015 World Congress on Industrial Control Systems Security (WCICSS), London, UK, 14–16 December 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 45–49. Song, H.M.; Kim, H.R.; Kim, H.K. Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network. In Proceedings of the 2016 International Conference on Information Networking (ICOIN), Kota Kinabalu, Malaysia, 13–15 January 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 63–68.

[16] Müter, M.; Asaj, N. Entropy-based anomaly detection for in-vehicle networks. In Proceedings of the 2011 IEEE Intelligent Vehicles Symposium (IV), Baden-Baden, Germany, 5–9 June 2011; pp. 1110–1115.

[17] Marchetti, M.; Stabili, D.; Guido, A.; Colajanni, M. Evaluation of anomaly detection for in-vehicle networks through information-theoretic algorithms. In Proceedings of the 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI), Bologna, Italy, 7–9 September 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–6.

[18] Wu, W.; Huang, Y.; Kurachi, R.; Zeng, G.; Xie, G.; Li, R.; Li, K. Sliding window optimized information entropy analysis method for intrusion detection on in-vehicle networks. IEEE Access 2018, 6, 45233–45245.

[19] Seo, E.; Song, H.M.; Kim, H.K. Gids: Gan based intrusion detection system for in-vehicle network. In Proceedings of the 2018 16th Annual Conference on Privacy, Security and Trust (PST), Belfast, Ireland, 28–30 August 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.

[20] Alshammari, A.; Zohdy, M.A.; Debnath, D.; Corser, G. Classification approach for intrusion detection in vehicle systems. Wirel. Eng. Technol. 2018, 9, 79–94.

[21] Bozdal, M.; Samie, M.; Jennions, I.K. WINDS: A wavelet-based intrusion detection system for Controller Area Network (CAN). IEEE Access 2021, 9, 58621–58633.

[22] Derhab, A.; Belaoued, M.; Mohiuddin, I.; Kurniawan, F.; Khan, M.K. Histogram-Based Intrusion Detection and Filtering Framework for Secure and Safe In-Vehicle Networks. IEEE Trans. Intell. Transp. Syst. 2021, 23, 2366–2379.

[23] Faruqui, N.; Yousuf, M.A.; Whaiduzzaman, M.; Azad, A.; Barros, A.; Moni, M.A. LungNet: A hybrid deep-CNN model for lung cancer diagnosis using CT and wearable sensor-based medical IoT data. Comput. Biol. Med. 2021, 139, 104961.

[24] Wójcicki, K.; Biega ´nska, M.; Paliwoda, B.; Górna, J. Internet of Things in Industry: Research Profiling, Application, Challenges

and Opportunities—A Review. Energies 2022, 15, 1806.

[25] Hasan, M.K.; Akhtaruzzaman, M.; Kabir, S.R.; Gadekallu, T.R.; Islam, S.; Magalingam, P.; Hassan, R.; Alazab, M.; Alazab, M.A. Evolution of industry and blockchain era: Monitoring price hike and corruption using BIoT for smart government and industry 4.0. IEEE Trans. Ind. Inform. 2022, 18, 9153–9161.

[26] Zhao, Y.; Lian, Y. Event-driven Circuits and Systems: A Promising Low Power Technique for Intelligent Sensors in AIoT Era. IEEE Trans. Circuits Syst. II Express Briefs 2022, 69, 3122–3128.

[27] Soldatos, J.; Gusmeroli, S.; Malo, P.; Di Orio, G. Internet of things applications in future manufacturing. In Digitising the Industry Internet of Things Connecting the Physical, Digital and Virtual Worlds; River Publishers: Delft, the Netherlands, 2022; pp. 153–183.

[28] Sharma, R.; Arya, R. Security threats and measures in the Internet of Things for smart city infrastructure: A state of art. Trans. Emerg. Telecommun. Technol. 2022, 1, e4571

[29] Diksha Siddhamshittiwar. (2017). An Efficient Power Optimized 32 bit BCD Adder Using Multi-Channel Technique. International Journal of New Practices in Management and Engineering, 6(02), 07 - 12. https://doi.org/10.17762/ijnpme.v6i02.57

[30] Smit, S., Popova, E., Milić, M., Costa, A., & Martínez, L. Machine Learning-based Predictive Maintenance for Industrial Systems. Kuwait Journal of Machine Learning, 1(3). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/139

[31] Dhabliya, D., & Parvez, A. (2019). Protocol and its benefits for secure shell. International Journal of Control and Automation, 12(6 Special Issue), 19-23. Retrieved from www.scopus.com Dhabliya, D., & Sharma, R. (2019). Cloud computing based mobile devices for distributed computing. International Journal of Control and Automation, 12(6 Special Issue), 1-4. doi:10.33832/ijca.2019.12.6.01