IJIRAE: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 10, Issue 03, March 2023 https://www.ijirae.com/archives

Smart Intrusion Detection System for CAN Network Implemented using LSTM Strategy

Sanjay S Tippannavar*
Department of Electronics and Communication Engineering,
JSS Science and Technology University, Mysuru, India
Sanjayu2345@gmail.com
Vanditha M
Department of Electronics and Communication Engineering,
JSS Science and Technology University, Mysuru, India
vandithamogra@gmail.com
Prerana Nayak
Department of Electronics and Communication Engineering,
JSS Science and Technology University, Mysuru, India
24nayakprerana@gmail.com

Publication History
Manuscript Reference No: IJIRAE/RS/Vol.10/Issue03/MRAE10087
Research Article | Open Access | Double-blind Peer-reviewed | Article ID: IJIRAE/RS/Vol.10/Issue03/MRAE10087
Received: 14, March 2023 | Revised: 18, March 2023 | Accepted: 21, March 2023 Published Online: 31, March 2023
Volume 2023 | Article ID MRAE10087 https://www.ijirae.com/volumes/Vol10/iss-03/08.MRAE10087.pdf
Article Citation: Sanjay,Vanditha,Prerana (2023). Smart Intrusion Detection System for CAN Network Implemented using LSTM Strategy. IJIRAE:: International Journal of Innovative Research in Advanced Engineering, Volume 10, Issue 03 of 2023 pages 98-105 https://doi.org/10.26562/ijirae.2023.v1003.08
BibTeX sanjay2023smart
Academic Editor-Chief: Dr.A.Arul Lawrence Selvakumar, AM Publications, India

Abstract: In today's cars, communication between electronic control units is managed via the Controller Area Network (CAN) bus system. Nevertheless, the CAN bus system lacks means for authentication and authorisation, making it susceptible to attacks like denial-of-service, fuzzing, and spoofing. To identify and counteract CAN bus network intrusions, this study suggests an intrusion detection system based on a Long Short-Term Memory (LSTM) model. Extraction of attack-free data and attack injection produced the dataset used for testing and training. Findings show that the suggested LSTM model has a greater detection rate than the Survival Analysis approach and is efficient in defending current automobiles from assaults on the CAN bus network. The ability to identify these sorts of assaults is limited by the constraints of conventional intrusion detection systems (IDS) for CAN bus networks, such as statistical analysis, frequency-based analysis, and Hidden Markov Model (HMM). Using a Long Short-Term Memory (LSTM) based strategy, the objective of this article is to build a reliable IDS that can efficiently identify and counteract these assaults on the CAN bus network.

Keywords: Automotive Networking, Cars, Safety, Intrusion detection, CAN, Attacks, DoS, LSTM, ML, Communication, Signal processing, Spoofing, Fuzzing.

I. INTRODUCTION

Modern vehicles include a central system for coordinating communication amongst electronic control units (ECUs), known as the Controller Area Network (CAN) bus system. CAN was created in the 1980s to provide a dependable and effective method for many ECUs to interact with one another. Using an Intrusion Detection System is one technique to defend contemporary vehicles against these assaults (IDS). IDS may be divided into four basic groups: hybrid, anomaly-based, misuse-based, and signature-based. Whereas anomaly-based IDS identifies odd or abnormal network behaviour, signature-based IDS employs pre-defined patterns or signatures to identify known threats. Misuse-based IDS incorporates the techniques of the other forms of IDS, whereas hybrid IDS compares network activity to a set of predetermined rules to identify known attack behaviours. In order to identify and counteract assaults on the CAN bus network, we suggest an IDS based on Long Short-Term Memory (LSTM) in this study.

Recurrent neural networks (RNNs) of the LSTM kind are good for seeing patterns in sequential data, making them suitable for spotting assaults on the CAN bus network. The Denial of Service (DoS), Fuzzing, and Spoofing assaults that may affect the CAN bus network are the three kinds of attacks that are the subject of this research. DoS attacks try to stop the network from functioning normally by flooding it with many requests or messages. Fuzzing attacks aim to produce mistakes or crashes by flooding the network with random or erroneous data. Spoofing attacks entail pretending to be a trustworthy network node and sending erroneous or malicious signals. By examining the sequence of communications on the network and spotting unexpected or aberrant behaviour, LSTM-based IDS is effective in recognising various sorts of assaults.

In-vehicle networks, particularly the Controller Area Network (CAN) bus, are being used more often, which has raised concerns about their security. A vital part of the design of a contemporary car is the CAN bus, which facilitates communication between different electronic control units (ECUs). The possibility of security breaches grows along with the number of ECUs in a vehicle. The CAN bus protocol is vulnerable to malicious attacks like Denial of Service (DoS), Fuzzing, and Spoofing because it lacks standardised security protections. Due to these problems, an efficient Intrusion Detection System (IDS) is urgently needed to identify and stop these assaults on the CAN bus network.

The major goal of this implementation is to strengthen automotive system security and guard against possible risks brought on by malicious assaults on the CAN bus network. Moreover, the goal is to determine how various hyper-parameter values affect the performance of the suggested IDS and to provide improved suggestions for fine-tuning the model for maximum effectiveness.

II. RECENT WORKS

For cars, intrusion detection systems (IDS) are a must, and unmanned, autonomous ones are especially vulnerable. Nevertheless, there hasn't been much work done to identify intrusions in an autonomous vehicle, and current IDSs aren't very effective against powerful attackers. As a result, Srivastava et al. suggest using the road context to create a Road context - aware IDS while also taking into account the basic nature of autonomous vehicles (RAIDS). The study makes the assumption that, in the case of a computer-controlled automobile, the pattern and data of frames communicated on the in-vehicle communication network should be reasonably predictable and accessible while the vehicle is travelling through continuous road situations. As a result, it has been designed RAIDS and implemented a basic prototype that recognises and distinguishes anomalous frames created or suspended by enemies. The findings of the evaluation demonstrate that RAIDS is capable of detecting intrusions that modern IDS are unable to **[1]**.

The security concerns of in-vehicle networks have significantly increased as a result of the expansion of contemporary cars' complexity and connectedness (IVNs). Yet current IVN designs, like the controller area network, don't take cybersecurity into account. This problem is addressed by intrusion detection, a powerful technique that ensures functional safety and real-time communication while thwarting cyberattacks on IVNs. Thus, the need for its investigation has increased. The limitations and features of an intrusion detection system (IDS) architecture for IVNs are provided by Wu et al. who also established the IVN environment. The disadvantages associated with the suggested IDS designs for the IVNs are surveyed and emphasised. Several optimization goals are taken into account and thoroughly contrasted. Finally, the trend, unresolved problems, and new prospects for study are outlined **[2]**.

A current area of study in the automobile industry is the creation of comprehensive IT security concepts due to the rising connection and seamless integration of information technology into contemporary cars. Because to its reactive nature, which enables it to respond to threats in real time, vehicle attack detection is one notion within this development that is receiving more attention. Asaj et al. investigate the viability of entropy-based attack detection for in-vehicle networks in this research. We highlight the essential components for applying such a strategy to the automobile industry. Applying the methodology to data obtained from a typical vehicle's CAN-Body network yields the first illustrative results **[3]**.

Computer networks are used to control contemporary vehicles. Formerly, there was little worry about the security of these networks, but in recent years, researchers have shown how vulnerable they are to several attacks. We test an anomaly detector for the automobile controller area network (CAN) bus as part of a defence against these assaults. A large percentage of attacks operate by adding additional packets to the network. However the majority of typical packets come at a fixed frequency. An anomaly detector that contrasts present-day and earlier packet timing is motivated by this. An approach for measuring inter-packet time across a sliding window is presented by Taylor et al. To detect anomalies, the average timings are contrasted with historical averages. The efficacy of this strategy is evaluated across a variety of insertion frequencies, and its limitations are shown. Finally, research demonstrates how a one class support vector machine can utilise the same data to confidently identify abnormalities **[4]**.

The in-vehicle CAN (Controller Area Network) bus network is vulnerable to major network security threats because it lacks network security protections. Nevertheless, due to the resource-constrained ECUs, the majority of intrusion detection methods necessitating substantial computing resources cannot be deployed in in car network system. In order to use cloud computing or add more hardware, we must address the cost issue as well as the necessity for reliable connection between cars and the cloud platform, which is challenging to do quickly. As a result, we must provide a temporary fix for the car industry. In this research, Jin et al. suggest an immediate and direct application of a signature-based lightweight intrusion detection system to automobile ECUs (Electronic Control Units). We identify the CAN bus abnormalities brought on by various attack techniques from real-world circumstances, which serve as the foundation for choosing signatures. The results of our experiments demonstrate the effectiveness of our strategy for finding abnormalities in CAN traffic. By taking use of the link between the signals, the detection ratio for anomalies related to content may be increased **[5]**.

Modern computer and communication technologies are being integrated into vehicles to transform them and enhance user experience and driving safety. As a consequence, formerly closed vehicle systems are now opening up to the outside world via different interfaces like Bluetooth, 3G/4G, GPS, etc., creating new potential for cyber attacks.

Modern automobiles have recently been shown to be susceptible to a number of remote assaults performed over Bluetooth and cellular connections, giving the attacker complete control of the target vehicle. Lack of message authentication for the vehicle's internal bus system, known as the Controller Area Network, is a typical cause of these assaults (CAN) [6].

As a de facto serial communication standard for cars, CAN bus offers an effective, trustworthy, and affordable connection between Electronic Control Units (ECU). Nevertheless, the CAN bus lacks sufficient security mechanisms to defend itself against intrusions from the inside or the outside. One of the greatest methods to raise the degree of vehicle security is using an intrusion detection system (IDS). Because of the limited computer capacity of the electronic equipment used in automobiles, IDS for vehicles must utilise a light-weight detection method as opposed to the typical IDS for network security. The study of CAN message time intervals is used by Song et al. to provide a lightweight intrusion detection system for in-vehicle networks. Work conducted three different types of message injection assaults on CAN messages taken from vehicles produced by a well-known manufacturer. As a consequence, it has been discovered that the time interval is a useful attribute for detecting assaults in CAN communications [7].

New attacks and vulnerabilities are developing as cars incorporate additional software modules and external connections. Several defence strategies have been put out to address these vulnerabilities, but they fall short of providing the robust defence that safety-critical ECUs require against in-vehicle network intrusions. Cho et al. offer the Clock-based IDS, an anomaly-based intrusion detection system (IDS), to address this shortcoming (CIDS). It detects frequent in-vehicle communication intervals and uses them to fingerprint ECUs. The Recursive Least Squares (RLS) technique is then used to build a baseline of the clock behaviours of ECUs using the thusly generated fingerprints. Based on this baseline, the Cumulative Sum (CUSUM) algorithm is used by CIDS to identify any anomalous changes in the identification errors, which are a blatant indication of intrusion. With a low false-positive rate of 0.055%, in-vehicle network breaches may be quickly identified. In contrast to cutting-edge IDSs, CIDS's fingerprinting of ECUs makes it easier to conduct a root cause investigation and determine which ECU launched the attack in the event that one is discovered [8].

In this article, Wolf et al. identified many issues with bus communication security while also providing a quick overview of existing and prospective vehicular communication systems. The majority of the local vehicular communication security issues are addressed using a method that leverages contemporary communication security methods. The most advanced cars will soon include multimedia buses and wireless connection interfaces. Malicious attackers are a genuine concern that should not be ignored, as is the case with current internet activity. This is especially true given that even a single successful assault with very minimal risks to passengers may substantially undermine public trust in a brand. Future automotive systems and business models, in particular, rely on thorough and effective measures that allow secure vehicular communication, thus the necessary technological, organisational, and financial arrangements must be made now [10].

Gmiden et al. suggested a straightforward intrusion detection approach for CAN bus IDS in this paper. The mechanism is based on the examination of CAN message time intervals. Implementing an IDS that first determines the CAN ID of the sent message and then determines the time intervals based on the most recent one is the major goal. In this book, a broad review of assaults, their categorization, and some strategies to protect against them are also included. The benefit of the strategy is that it may be implemented in each ECU without changing the hardware layer [11].

III. METHODOLOGY

Using an Intrusion Detection System is one technique to defend contemporary vehicles against these assaults (IDS). IDS may be divided into four basic groups: hybrid, anomaly-based, misuse-based, and signature-based. Whereas anomaly-based IDS identifies odd or abnormal network behaviour, signature-based IDS employs pre-defined patterns or signatures to identify known threats. Misuse-based IDS incorporates the techniques of the other forms of IDS, whereas hybrid IDS compares network activity to a set of predetermined rules to identify known attack behaviours. It has also been suggested to use GAN-based IDS, which have achieved attack detection rates of 99.60%, 99.50%, 99.00%, and 96.50%. There have also been other approaches put forward, including Survival Analysis, unsupervised deep belief networks (DBN), and artificial neural networks (ANN). Moreover, researchers have proposed IDS for in-vehicle networks based on time interval analysis (TIA) and request-response message analysis and employed various machine learning algorithms to categorise CAN bus data. In this part, we discovered that for intrusion detection in in-vehicle networks, deep learning algorithms like Long Short-Term Memory (LSTM) outperform other approaches (CAN bus). Statistical analysis, frequency-based analysis, and Hidden Markov Model are some of these approaches (HMM). The LSTM-based IDS for CAN bus networks that we present in this research is anticipated to perform better than earlier work since the hyper-parameter values have been adjusted.

In this research, we provide an IDS that uses Long Short-Term Memory (LSTM) to identify and counteract assaults on the CAN bus network. Recurrent neural network (RNN) LSTM is effective at seeing patterns in sequential data, which makes it a good choice for spotting assaults on the CAN bus network. This document discusses the three most frequent forms of assaults that might target the CAN bus network: spoofing, fuzzing, and denial of service (DoS).

- DoS Attack: Attacking the network with a huge volume of requests or messages is known as a denial of service (DoS) attack, which seeks to prevent it from operating normally. This kind of attack may result in an increase of unneeded traffic on the network, which will lower the system's overall performance.

- Sending several messages with a high priority level to a CAN network may be used to conduct a DoS attack, which may result in the blocking of other crucial communications. This kind of assault on automotive systems has the potential to have devastating effects including car crashes, engine failure, etc.
- Fuzzing Attack: Sending random or erroneous data to a Controller Area Network (CAN) system in an effort to trigger faults or crashes is known as fuzzing. By taking advantage of flaws in how the system processes improper input, fuzzing attacks seek to find vulnerabilities in the system. Fuzzing attacks often employ a large number of random inputs and are automated to test the system's reaction.
- Spoofing attack: Attacks that imitate genuine network nodes in order to send erroneous or harmful signals are known as spoofing attacks on Controller Area Network (CAN) systems. A spoofing attack aims to introduce false or misleading information into the system in order to obtain unauthorised access to it or to interfere with the network's regular functioning. An attacker may start a spoofing attack in a CAN network by intercepting or sniffing the communication and then replaying it, changing the message, or sending a bogus message with a legitimate identity.

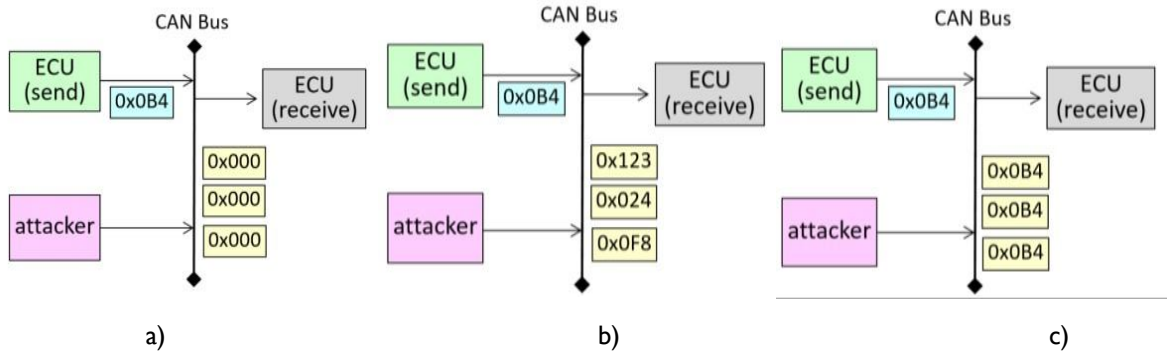

Fig.1.Attack scenarios assumed in this paper. (a) DoS attack – an attacker floods messages to the CAN bus. (b) Fuzzing attack – an attacker injects random CAN messages for changing the IDs, payload length. (c) Spoofing attack – an attacker generates fake messages that deceive the receiver's ECUs.

A Long Short-Term Memory (LSTM)-based intrusion detection system (IDS) for the Controller Area Network (CAN) bus network is part of the implementation scope for this project. Attacks such as Denial of Service (DoS), Fuzzing, and Spoofing attacks would be able to be detected and mitigated by the proposed IDS against the CAN bus network.

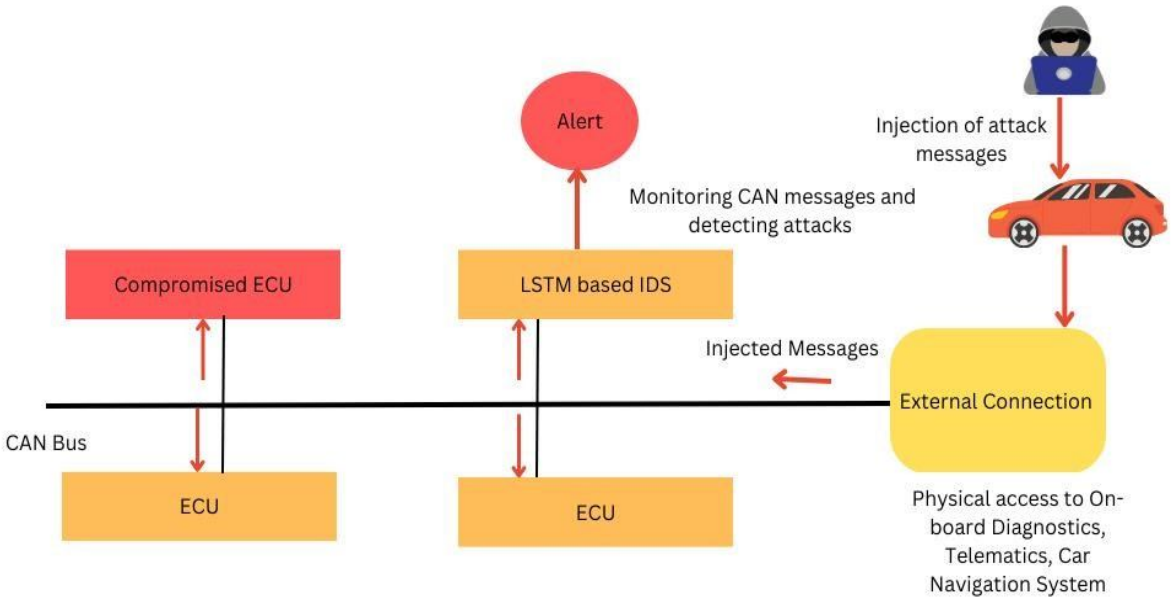

Fig.2. Architecture of the proposed system for a CAN network.

A backward-compatible authentication method or the creation of an Intrusion Detection System are the two most apparent ways to stop assaults on the CAN bus system (IDS). The CAN bus system of a car is under assault, and an IDS based on Long Short-Term Memory (LSTM) is presented in this research to identify the attacks.

ISSN: 2349-2163
https://www.ijirae.com/archives

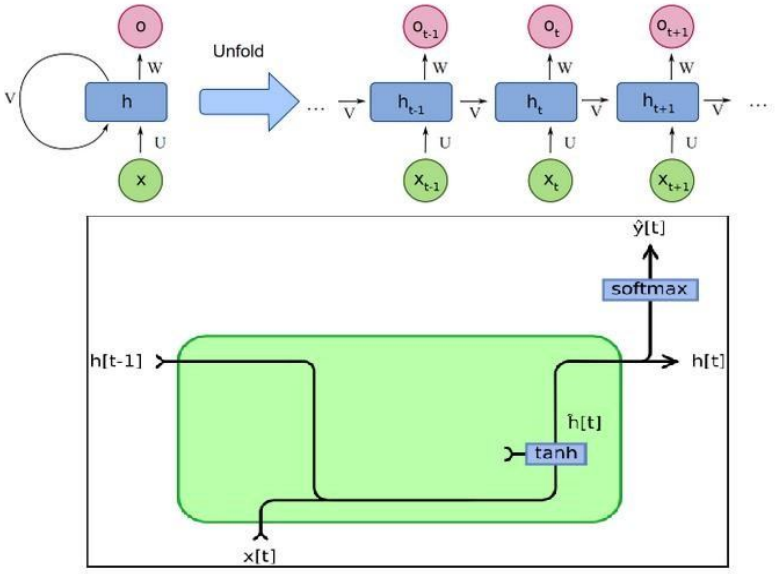

Fig.3. Basic RNN structure

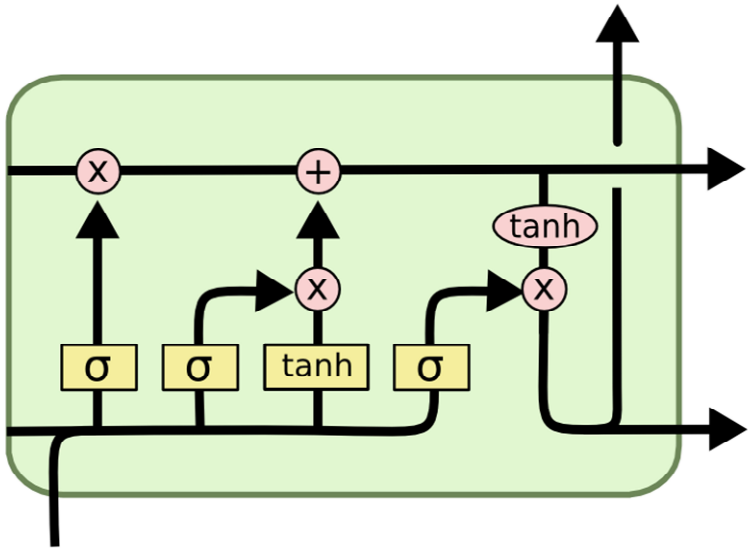

Fig.4. Basic LSTM network

In the work, an Autoencoder model for CAN system anomaly detection is put into practise. Data on CAN IDs, payloads, and time intervals are included in the NAIST CAN dataset, which is used in this research. Unsupervised learning models like the autoencoder model, which is taught to recreate its input data, fall under this category. The rationale for employing an autoencoder for anomaly detection is that although the model should readily recreate normal data, aberrant data will produce a larger reconstruction error.

Processing the dataset is the first stage of project implementation. The priority, function, subfunction, node id, payload length, and payload data are among the columns that are chosen from the dataset when it is read in as a CSV file. Then, using a Min-Max Scaler to normalise the values in these columns, the hexadecimal data is transformed to decimal. An initial training set and a subsequent test set are created from the processed data. With the training set, the autoencoder model is created and trained. Encoder and decoder components make up the model. The input data is compressed by the encoder into a lower-dimensional representation, and the decoder makes an effort to recreate the original data from this representation. The difference between the original data and the rebuilt data is measured and used to train the model using the mean absolute error (MAE) loss function.

After training, predictions are made using the test set using the model. After then, the predictions are evaluated against the data from the first test set to determine the reconstruction error. After a threshold has been established to separate normal data from abnormal data, this reconstruction error is utilised as a measure of abnormality. The data from the test set are shown as a scatter plot as a consequence, with points that are over the threshold being classified as anomalies. In the project's implementation, the autoencoder is utilised to find anomalies in the NAIST CAN dataset, which may be used to find anomalous behaviour in CAN systems in real-world settings. It is feasible to stop larger issues from developing and guarantee the system's efficient functioning by spotting these irregularities early.

Layer (type)	Output Shape	Param #
input_1 (InputLayer)	[(None, 1, 13)]	0
lstm (LSTM)	(None, 1, 16)	1920
lstm_1 (LSTM)	(None, 4)	336
repeat_vector (RepeatVector)	(None, 1, 4)	0
lstm_2 (LSTM)	(None, 1, 4)	144
lstm_3 (LSTM)	(None, 1, 16)	1344
time_distributed (TimeDistributed)	(None, 1, 13)	221

Total params: 3,965
Trainable params: 3,965
Non-trainable params: 0

Fig.5. Architecture of the Autoencoder model.

A specific kind of unsupervised neural network called an autoencoder is taught to recreate its input. It comprises of an encoder and a decoder that translate the input data into a lower-dimensional representation (sometimes referred to as the bottleneck or latent representation) and translate the lower-dimensional representation back to the original input space. The autoencoder is taught to reduce the reconstruction error, which is the difference between the input and the reconstructed output. Dimensionality reduction, data denoising, and anomaly detection are a few examples of the tasks that autoencoders may be utilised for. The autoencoder is trained on typical data for anomaly detection, and then the reconstruction error is calculated for fresh, unused data. The likelihood of the new data being aberrant or an anomaly increases with a significant reconstruction error. For models of the autoencoder type, accuracy metrics are inappropriate. The mean absolute error (MAE) loss function is used to train the model and quantifies the discrepancy between the expected and actual output. To make the model's output as similar to the genuine output as feasible, the training procedure aims to reduce this disparity as much as possible. Moreover, the model is not utilised for classification but rather for reassembling the input data, hence accuracy is not utilised.

IV. RESULTS AND DISCUSSIONS

Fig. 6 shows the mean absolute error (MAE) between the predicted values and the actual values, which is used to determine the loss for the training set.

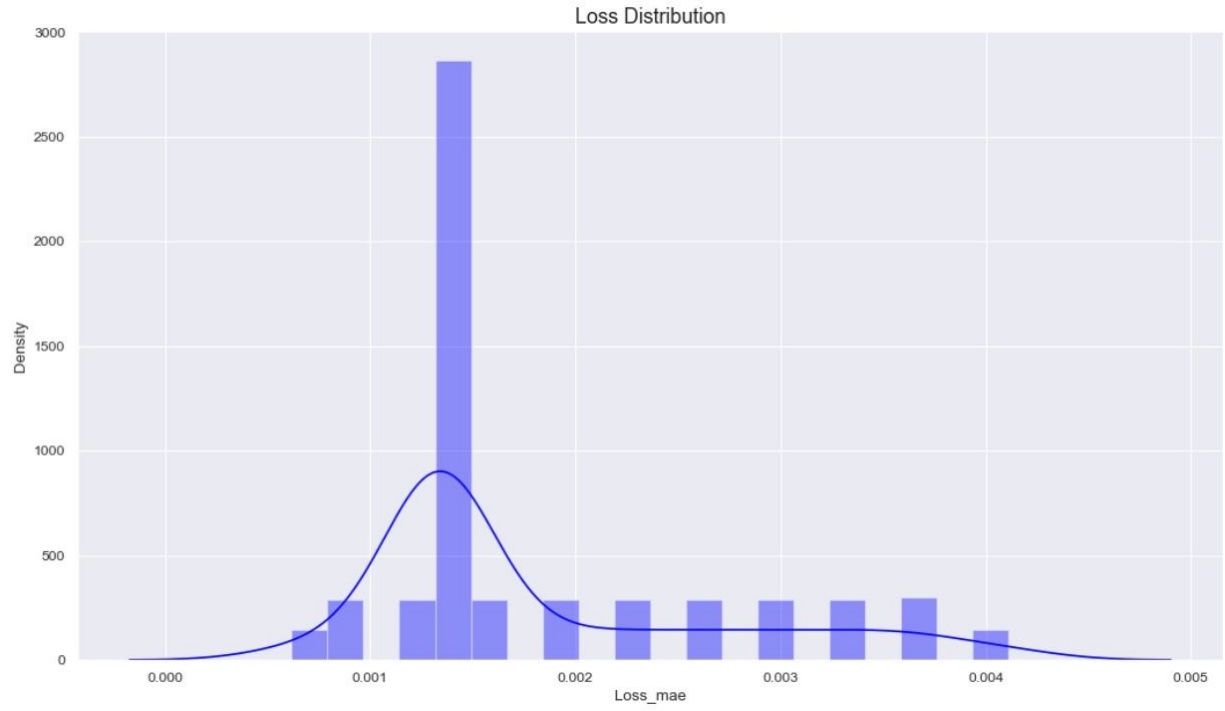

Fig.6. Plot of Reconstruction Error

The index of the observations in the training set is shown on the x-axis. The distribution of the Loss MAE values generated for each observation in the training set is shown on the figure. The values are represented on a logarithmic scale since the y-axis is on a log scale. The distribution of the Loss MAE, which indicates the mean absolute error between the original values and the predicted values of the Auto encoder, is inferred from the figure. A lower Loss MAE number indicates that the auto encoder has learnt important features from the training data since it can recreate the original input values more precisely.

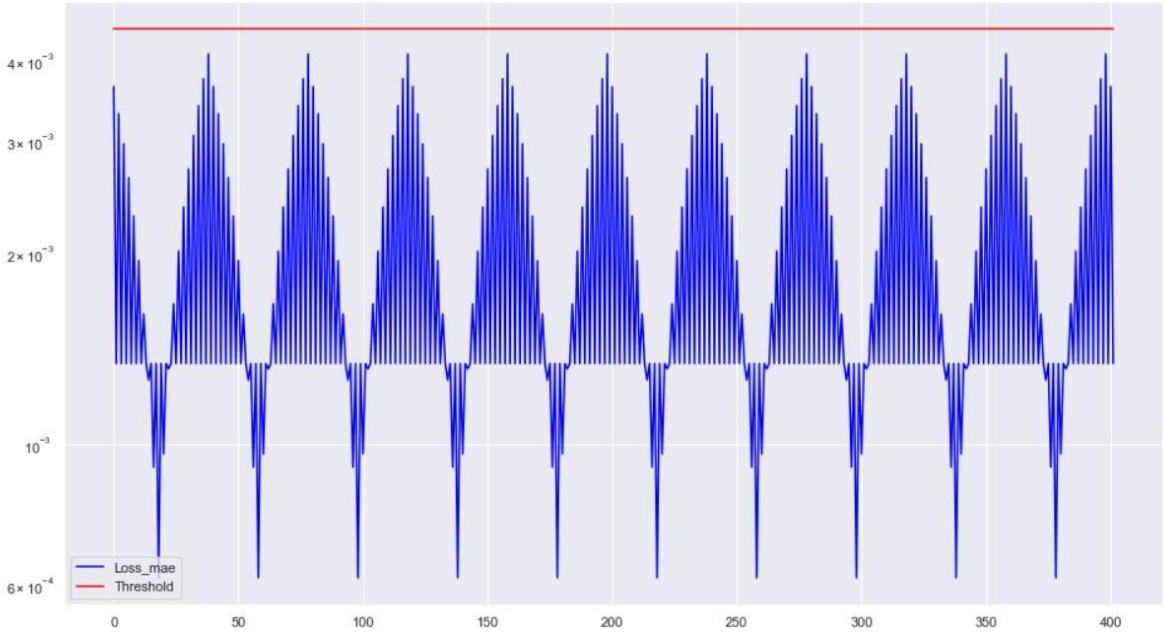

Fig.7. Bearing Failure Time Plot

Using the data points' indexes on the x-axis and mean absolute error on the y-axis, the graphic shows the discrepancy between the expected and actual values of the data. Fig. 7 depicts the Bearing Failure Time plot, a threshold line separating the regular data from the abnormal data is also shown on the graphic. The divergence from a set threshold is deemed to be greater for the points over the threshold line, which indicates a probable failure.

V. CONCLUSIONS

For identifying and thwarting assaults on the Controller Area Network (CAN) bus network, this research concludes by presenting an intrusion detection system (IDS) based on Long Short-Term Memory (LSTM). We successfully identified patterns in sequential data using LSTM, a form of Recurrent Neural Network (RNN), with acceptable accuracy for benign and attack cases and low false positive and false negative detection rates. The three primary forms of attacks on the CAN bus network Denial of Service (DoS), Fuzzing, and Spoofing were able to be found and categorised by the suggested IDS.
Future study in a number of areas might broaden its current coverage, including:

1. Examine the performance of the proposed LSTM-based IDS in actual automotive systems and contrast it with other IDSs already in use.
2. In addition, the suggested IDS may be expanded to include several kinds of network-level attacks, such Man-in-the-Middle (MitM) and Replay assaults.

REFERENCES

1. Tanya Srivastava, Pryanshu Arora, Chundong Wang, Sudipta Chattopadhyay, "Work-in-Progress: Road Context-aware Intrusion Detection System for Autonomous Cars", 2018 https://doi.org/10.1109/emsoft.2018.8537210
2. W. Wu, R. Li, et al. "A survey of intrusion detection for in-vehicle networks," IEEE Transactions on Intelligent Transportation Systems, 2019, pp. 919-933
3. M. Müter and N. Asaj, "Entropy-based anomaly detection for in vehicle networks," IEEE Intelligent Vehicles Symposium (IV), Baden-Baden, 2011, pp. 1110-1115 https://doi.org/10.1109/ivs.2011.5940552
4. Taylor, N. Japkowicz and S. Leblanc, "Frequency-based anomaly detection for the automotive CAN bus," 2015 World Congress on Industrial Control Systems Security (WCICSS), London, 2015, pp. 45- 49 https://doi.org/10.1109/wcicss.2015.7420322
5. Shiyi Jin, Jin-Gyun Chung, Yinan Xu, "Signature-Based Intrusion Detection System (IDS) for In-Vehicle CAN Bus Network", 2021 IEEE International Symposium on Circuits and Systems (ISCAS) https://doi.org/10.1109/iscas51556.2021.9401087
6. Q. Wang, S. Sawhney, "VeCure: A Practical Security Framework to Protect the CAN Bus of Vehicles", 2014. https://doi.org/10.1109/iot.2014.7030108
7. H. M. Song, H. R. Kim and H. K. Kim, "Intrusion Detection System Based on the Analysis of Time Intervals of CAN Messages for In Vehicle Network", 2016. https://doi.org/10.1109/icoin.2016.7427089

8. K-T. Cho, K.G. Shin," Fingerprinting Electronic Control Units for Vehicle Intrusion Detection", 2016
9. Rajkumar Singh Rathore, Chaminda Hewage, Omprakash Kaiwartya, Jaime Lloret, "In-Vehicle Communication Cyber Security: Challenges and Solutions", Sensors 2022 https://doi.org/10.3390/s22176679
10. M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," Workshop on Embedded Security in Cars, 2004 https://doi.org/10.1007/3-540-28428-1_13
11. Sanjay S Tippannavar, Raghavendra G, Rishab Jain, Prasanna Golasangi."SPF: Smart Pet Feeder using IoT for Day-to-Day Usage", Volume 11, Issue I, International Journal for Research in Applied Science and Engineering Technology (IJRASET) Page No: 299-304, ISSN : 2321-9653. https://doi.org/10.22214/ijraset.2023.48403
12. Sanjay S Tippannavar, Surya M S, Pilimgole Sudarshan Yadav , Mohammed Zaid Salman, Ajay M."Hand Gesture based Speech Recognition system for Hard of Hearing People", Volume 10, Issue XI, International Journal for Research in Applied Science and Engineering Technology (IJRASET) Page No: 545-551, ISSN : 2321-9653, https://doi.org/10.22214/ijraset.2022.47301
13. S. S. Tippannavar, S. B. Rudraswamy, S. Gayathri, S. P. Kulkarni, A. Thyagaraja Murthy and S. D. Yashwanth, "Smart Car - One stop for all Automobile needs," 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 2022, pp. 54-59,https://doi.org/10.1109/icccis56430.2022.10037715
14. Tippannavar, Sanjay & Jain, Sourab & Harshith, R & Chandanagiri, Sweekar. (2022). IMAGE PROCESSING BASED INTELLIGENT TRAFFIC CONTROL SYSTEM USING OPENCV. 10. 2320-2882. 10.1729/Journal.32457.
15. Tippannavar, Sanjay. (2022). Land Mine Detection Robot using BLE-3.0 Voice Controlled, using Joystick and Gyroscopic sensor. 7. 609-614. 10.5281/zenodo.7493483.