IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

National Level Conference – AITCON 2K25

Adarsh Institute of Technology & Research Centre, Vita, Maharashtra

Vol. 12, Special Issue 1, March 2025

Enhancing Cyber Attack Detection with Machine Learning through Multi-Objective and Evolutionary Optimization for autonomous vehicles

Ms. Rahin Ismail Tamboli[1], Prof.V.D.Desai[2]

Student, CSE, Ashokrao Mane Group of Institution Vathar, Maharashtra India[1]

Professor, CSE, Ashokrao Mane Group of Institution Vathar, Maharashtra India[2]

Abstract: The automobile industry has seen a major upheaval since the introduction of electric vehicles (EVs), which provide a sustainable substitute for traditional internal combustion engine automobiles. However, because EVs are more closely linked to digital technologies, they are more vulnerable to hacking. The attacks can give the more hazard to EV owners because of safety concern. This paper gives the how machine learning techniques including the multi-objective optimization can be used to identify and reduce cyberattacks on electric vehicles. the fusion of unsupervised techniques like auto encoders and isolation forests with supervised machine learning algorithms like ANN and LSTM. The large number of data from EV component, control unit and communication network are gathered and analysed. The unsupervised algorithms use anomaly detection to identify new or emerging threats, while supervised algorithms are trained on labelled datasets to classify current types of cyber-attacks. The suggested model's performance is assessed using a real dataset. This study emphasizes how important machine learning technique and multi-objective optimization is to protecting the future generation of electric vehicles from new threats and guaranteeing their safe and reliable operation.

Keywords: Machine Learning, Electric Vehicle, Cyber Attack, Security

I. INTRODUCTION

The current Electric vehicles (EVs) incorporate digital technologies for the improvement of user experience, connectivity and reliable performance. The more important step of future generation of EV is friendly and sustainable transportation is represented by EV. The many types of Cyber-attacks are done on EV because of integration of Integration of Internet of Things(IOT) and smart software systems. The attacker can target the electric vehicles have some potential to cause serious issues such as altering control and gaining access to important information. Infrastructure damaging that facilitates charging, and endangering the safety of the passengers. EV are networked and depends upon some communication networks for number of operation including remote diagnostics, navigation, and battery management, hackers find them to be appealing targets. [1] Since normal cybersecurity measures are frequently insufficient to solve the particular difficulties posed by the automotive sector, the specific vulnerabilities of electric vehicle (EV) systems frequently need the development of innovative solutions. In this situation, machine learning (ML) and optimization provides a useful method to improve the identification and defends the cyber-attacks that are targeting the electric vehicles. The Large amounts of data produced by EV components may be analysed in real-time by ML algorithms, which enables the identification of patterns and anomalies that might point to a possible cyberthreat. Machine learning is a valuable technique for creating strong cybersecurity frameworks because of its many benefits, including its capacity to learn from past data and adjust to novel attack types. This study investigates how machine learning techniques might be used to detect cyberattacks on electric vehicles. The suggested method entails gathering and examining data from a number of EV subsystems, such as control units, communication networks, and battery management systems. [2]. The suggested method can use the ANN LSTM algorithm and multi-objective optimization for detection cyber-attack on control data.

II. LITERATURE SURVEY

Cyberattacks that jeopardize the security and functionality of electric vehicles (EVs) are more common. Checkoway et al. [1] demonstrated how cellular networks and Bluetooth interfaces may be used to remotely exploit internal automotive systems. Important safety issues were raised by Miller and Valasek [2], who also provided more examples of the possibility of remote control vehicle operations. Our findings highlight the importance of having strong cybersecurity protections against a range of attack vectors, including internal systems, communication networks, and charging infrastructure, in order to safeguard EVs. An essential cybersecurity strategy is anomaly detection, which looks for departures from the usual that can indicate a security issue.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

National Level Conference – AITCON 2K25

Adarsh Institute of Technology & Research Centre, Vita, Maharashtra

Vol. 12, Special Issue 1, March 2025

Chandola and associates offered a thorough analysis of anomaly detection methods, highlighting its use in a variety of fields, such as network security. The implementation of more dynamic solutions, such as machine learning, is necessary since statistical and rule-based approaches, despite their widespread use, typically fall short of the constantly changing nature of cyber threats. In order to improve cybersecurity defences, machine learning (ML) has become crucial. In their assessment of the use of machine learning (ML) for network intrusion detection, Buczak and Guven [4] pointed out that algorithms like Support Vector Machines (SVM) and Random Forests are useful for categorizing hostile activity. In their evaluation of the benefits and difficulties of implementing machine learning (ML) in network intrusion detection systems, Sommer and Paxson [5] emphasized the necessity of ongoing adjustment and learning from fresh data. Machine learning applications for EV cybersecurity have been the subject of numerous investigations. For connected and self-driving cars, Gao et al. [6] presented an intrusion detection system based on machine learning that can spot anomalies in vehicle communication data. Deep learning techniques are used in this system. Zhang et al. created a machine learning framework that uses both supervised and unsupervised learning approaches in an effort to increase the accuracy of cyberattack detection on EV battery management systems. To find abnormalities, supervised learning techniques like Random Forest and Support Vector Machines (SVM) are frequently employed in cybersecurity. According to Cristianini and Shawe-Taylor [8], SVM can be utilized to differentiate between benign and malignant activities because it performs well on binary classification tasks. Breiman [9] presented Random Forest, a method that combines the output of many decision trees to decrease overfitting and enhance detection performance. These algorithms have demonstrated great potential in recognizing and categorizing cyberthreats in a variety of fields. Autoencoders and isolation forests are examples of unsupervised learning algorithms that are essential for identifying new or unknown assaults. Isolation Forest is useful for detecting irregularities because it isolates data in the feature space, as shown by Liu et al. [10]. Neural networks known as auto encoders can be used to learn data representations and use input reconstruction to find anomalies. Salakhutdinov and Hinton [11] talked about this method. These algorithms are very useful because they don't need labelled data to find underlying patterns and outliers. EV cybersecurity has made great strides, but there are still many issues. Because cyber threats are dynamic and sophisticated, detection techniques must be updated frequently. Furthermore, real-time processing and data standards are severely hampered by the integration of disparate data streams from different EV components. To guarantee the strong cybersecurity of electric vehicles, future research should concentrate on creating more flexible and thorough machine learning models, refining data integration strategies, and boosting real-time threat detection capabilities.

Table1 Comparative Analysis of Existing System

Paper Title and author	**Concept**	**Key Finding**	**Technique used**	**Advantage**	**Disadvantage**
Checkoway et al.'s thorough experimental analyses of automotive attack surfaces [1]	Internal system vulnerabilities in vehicles	demonstrated remote control via cellular networks and Bluetooth.	Analytical experimentation	emphasized the critical necessity for cybersecurity precautions	restricted to particular interfaces and without mitigating techniques
Miller and Valasek, Adventures in Automotive Networks and Control Units [2]	Controlling a car remotely	Poses potential for remote control, raising concerns about safety	Analytical experimentation	highlighted the important safety ramifications	proof-of-concept rather than scalable solutions in focus
Chandola et al., Anomaly Detection: A Survey [3]	Finding anomalies in cybersecurity	examined a range of anomaly detecting methods	Methods based on rules and statistics	thorough overview and cross-domain suitability	Conventional approaches are not flexible enough.

Buczak and Guven, A Survey of Data Mining and Machine Learning Techniques for Cyber Security Intrusion Detection [4]	ML for the detection of network intrusions	efficient in identifying harmful activity	Random Forest, SVM	Enhanced precision and flexibility	requires a lot of computing power and big databases.
Outside the Closed World: On Network Intrusion Detection Using Machine Learning, Paxson and Sommer [5]	ML in intrusion detection systems for networks	discussed the potential and difficulties of using ML in applications.	Machine Learning Algorithms	emphasized the necessity of ongoing adaptation	Real-world implementation difficulties
Gao et al. [6] presented a machine learning-based intrusion detection method for in-vehicle networks.	Vehicles that are linked and autonomous can detect intrusions.	A system based on deep learning is suggested to detect anomalies.	Deep learning methodologies	high real-time detection accuracy	high processing costs and intricate models
Zhang et al. [7] published Machine Learning-Based Cyber-Attack Detection for Electric Vehicle Battery Management Systems.	Cyberattack identification for electric vehicle battery management systems	supervised and unsupervised learning were used to develop the ML framework.	Different machine learning algorithms	improved detection precision, relevant to particular EV components	restricted to battery management; more widespread use is required
Cristianini and Shawe-Taylor, An Introduction to Support Vector Machines and Other Kernel-based Learning Methods [8]	SVM for identifying anomalies	efficient in problems involving binary classification	SVMs, or support vector machines	resilience and high classification accuracy	needs labeled data and is dependent on the parameter configuration

Hinton and Salakhutdinov, Reducing the Dimensionality of Data using Neural Networks [9]	Reducing dimensions and identifying anomalies	utilized autoencoders to learn about data representation	Encoders on autoencode	Effective in detecting anomalies without supervision	needs sophisticated training and fine-tuning.

III. PROPOSED SYSTEM

The proposed system enhances detection and response to cyberattacks on electric vehicles (EVs) by integrating machine learning techniques with multi-objective optimization within an advanced architecture. The design consists of several interconnected modules, each optimized to fulfil a specific security function efficiently. The data collection module gathers unprocessed data from sources such as network traffic, EV actuators, and sensors, covering systems like the battery management system, vehicle control, and communication interfaces. Network traffic data is also monitored to capture interactions between the EV and external entities like infrastructure, other vehicles, and charging stations, providing a comprehensive view to detect any anomalous activity. To streamline the analysis, optimization techniques are applied to the data pre-processing stage, eliminating noise, standardizing formats, and selecting relevant attributes for more precise machine learning outcomes. This optimized pre-processing allows for reduced computational load and improved accuracy in detecting potential threats. At the core of the system, NLP and ANN for identifying known attack patterns, such as Auto encoders and Isolation Forest, to detect novel or unknown threats. Multi-objective optimization is applied to select and tune these models, balancing detection accuracy with computational efficiency to ensure robust, real-time performance. An anomaly detection module continuously monitors optimized data flows and generates alerts for critical threats, assigning severity ratings based on optimized threat assessment criteria. This system enables rapid response actions that mitigate known threats efficiently, such as limiting vehicle functions, isolating affected components, or disabling certain systems to prevent damage. A logging module also records all anomalies and responses, supporting continuous optimization and improvement of security protocols, making the system adaptive and resilient against evolving cyber threats.

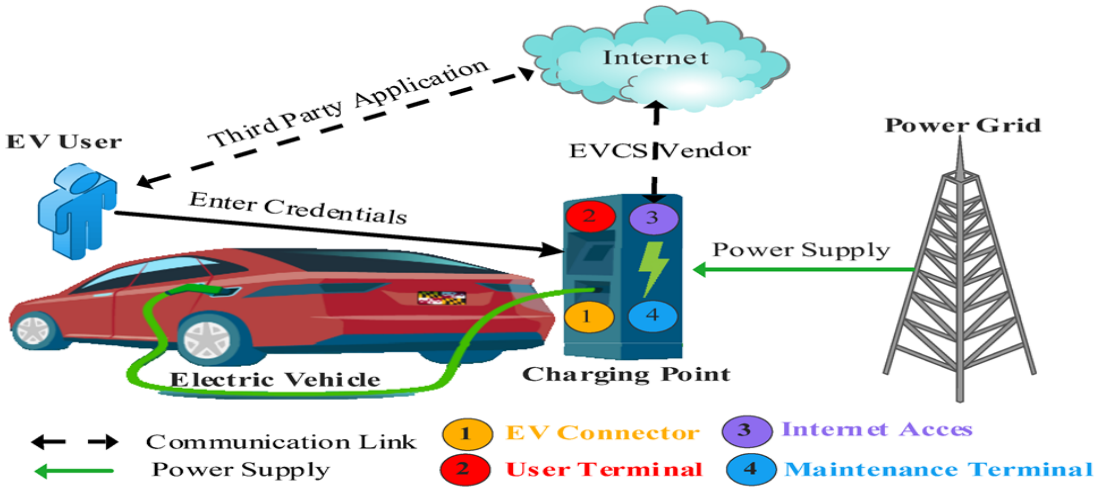


Fig1 . EVCSs with Vulnerable points

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

National Level Conference – AITCON 2K25

Adarsh Institute of Technology & Research Centre, Vita, Maharashtra

Vol. 12, Special Issue 1, March 2025

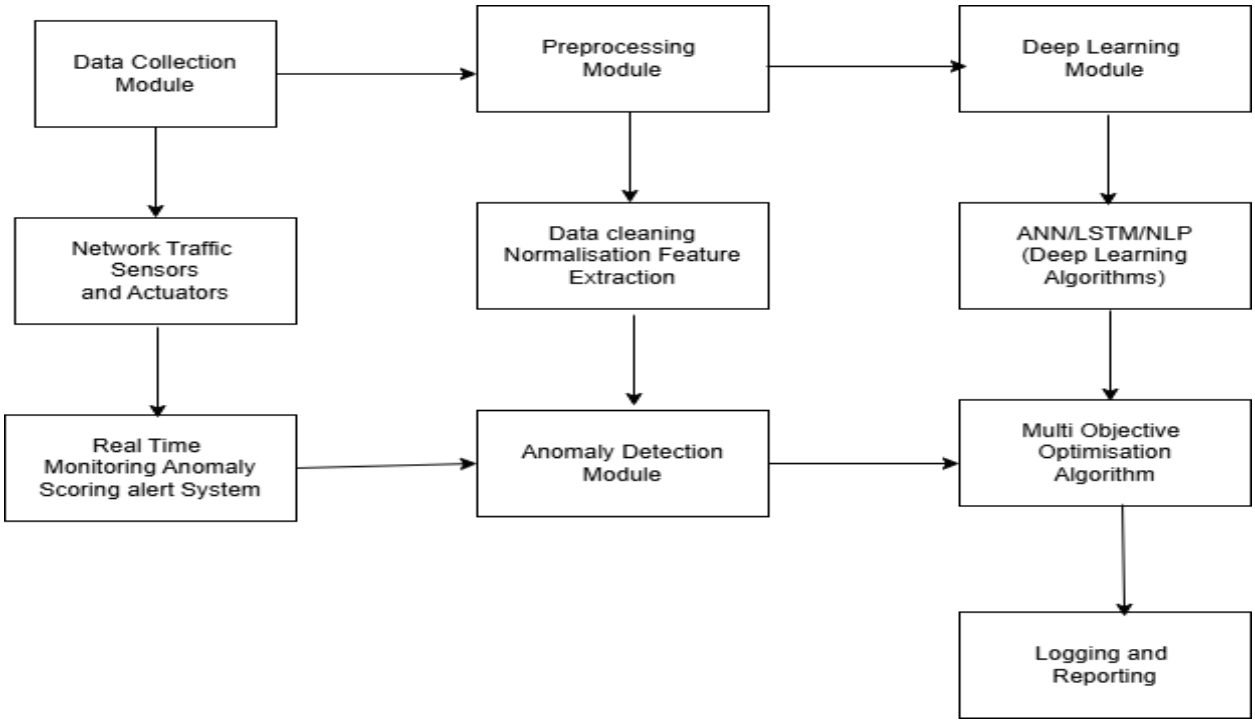


Fig2. Flow Diagram

IV. STEPS OF WORKING

Data Cleaning: This modules removes the noise from the data. Data cleaning removes noise or inconsistencies in the dataset. The data cleaning is done with extracting relevant parts (Timestamp, ID, DLC, Data) from the CAN log file using regular expressions and also it handling of unmatched lines by logging them into a separate file.

Normalization: This module can normalize the data for the preparation of machine learning. A data preprocessing method called normalization scales a dataset's numerical properties to a common range, usually between 0 and 1 or -1 and 1. Normalization's main objective is to make sure that every feature, independent of larger-scale features, contributes equally to the machine learning model's learning process. This is especially crucial when utilizing algorithms that depend on distance measuresas features with bigger scales might have an outsized impact on the outcomes. The eq(1) describes the normalization formula.

$$X_{\text{norm}} = \frac{X - X_{\text{min}}}{X_{\text{max}} - X_{\text{min}}} \qquad (1)$$

- **X**:

The actual value of a feature for a specific instance in the dataset.

- **Xmin**:

The smallest value (minimum) in the feature column. This is used to shift all values so that the minimum starts at 0.

- **Xmax**:

The largest value (maximum) in the feature column. This is used to scale all values proportionally so that the maximum ends at 1.

- **Xnorm**:

The normalized value of XXX, which will now be scaled to a range of 0 to 1.

Feature Extraction: The relevant features that machine learning models will use to detect abnormalities are gathered in this sub-module.Feature extraction derives new, relevant features from raw data to help the machine learning model detect abnormalities.
Time_Diff: The time difference between consecutive messages.
ID_Freq: Frequency of each ID.
Data_Byte_Count: Number of bytes in the data payload.

ANN

Artificial Neural Networks (ANNs) are highly beneficial for cyber attack detection because they excel at identifying complex patterns within large, high-dimensional data, like network traffic or system logs. In cybersecurity, this ability allows ANNs to detect subtle anomalies and deviations that may indicate malicious activity. ANNs process network data through layers of interconnected neurons, learning to distinguish between normal and suspicious behaviors. By training on extensive datasets that include both normal and attack behaviors, ANNs can classify real-time network activity and flag potential threats. Their adaptability also allows them to recognize previously unseen attack types, providing robust defenses against evolving cyber threats. With continuous monitoring, ANN-based systems reduce response times, enhancing cybersecurity by enabling rapid intervention when anomalies are detected. This proactive approach helps mitigate potential damage from cyber attacks, making ANNs a critical component in modern cybersecurity solutions.

Working On ANN Algorithm

Step 1: Data Collection

The `.txt` file containing network traffic data is read and parsed using a regular expression. The extracted fields include:
- Timestamp: Packet timestamp.
- ID: Packet identifier.
- DLC: Data Length Code (number of bytes in the data payload).
- Data: Hexadecimal payload of the packet.

Step 2: Data Preprocessing

1. Convert Timestamp and Compute Time Intervals:
- The `Timestamp` is converted to numeric format.
- Time intervals (`Time_Interval`) between consecutive packets are computed.
2. Hexadecimal Data Conversion:
- Hexadecimal payload (`Data`) is converted to an integer value (`Hex_Sum`) by summing up the byte values.
3. Packet Count Per ID:
- Count the number of packets for each `ID` (`Packet_Count`).
4. Time Window Aggregation:
- Group data into fixed time windows (e.g., 100 ms) and compute aggregated features:
  - Mean `DLC`.
  - Sum of `Time_Interval`.
  - Mean of `Hex_Sum`.
  - Total `Packet_Count`.
5. Generate Features and Labels:
- The aggregated features serve as input features (`X`).

Step 3: Splitting Data

The dataset is split into training and testing sets:
- Training Set: 80% of the data.
- Testing Set: 20% of the data.

Step 4: Feature Scaling

The features (`X`) are scaled using `StandardScaler` to normalize the data for better performance of the ANN.

Step 5: ANN Model Design

1. Input Layer:
- The input layer receives the preprocessed feature set with dimensions matching the number of input features.
2. Hidden Layers:
- First Hidden Layer:
  - 64 neurons with ReLU activation function.
- Second Hidden Layer:
  - 32 neurons with ReLU activation function.
3. Output Layer:
- Single neuron with a sigmoid activation function for binary classification (normal vs. attack).

Step 6: Compilation

The model is compiled with:
- Optimizer: Adam.

- Loss Function: Binary cross-entropy.
- Evaluation Metric: Accuracy.

Step 7: Model Training

The ANN is trained on the training set using:
- 20 epochs.
- Batch size of 32.

The model learns to classify normal and attack packets based on the input features.

Step 8: Prediction

Predictions are made on the test set. Sigmoid activation outputs probabilities, which are thresholded at 0.5 to classify as normal (0) or attack (1).

Step 9: Evaluation

1. Accuracy Calculation:
- Compare predicted labels with actual labels to compute accuracy.
2. Confusion Matrix:
- Evaluate model performance using a confusion matrix to identify:
  - True Positives.
  - True Negatives.
  - False Positives.
  - False Negatives.
3. Visualization:
- Plot a heatmap of the confusion matrix for better understanding of the results.

Step 10: Iteration and Tuning

LSTM

Long Short-Term Memory (LSTM) networks are particularly valuable in cyber-attack detection because they are designed to handle sequential data, making them ideal for analyzing time-series information like network traffic over time. Unlike traditional neural networks, LSTMs have a memory component that allows them to retain relevant information from earlier in the sequence, making them effective at identifying patterns and anomalies across time. This capability is crucial for detecting attacks that unfold gradually, such as data exfiltration, reconnaissance, or Distributed Denial-of-Service (DDoS) attacks, which may not be immediately identifiable from a single data point but reveal themselves through patterns over time. LSTM networks are trained on sequences of network events, enabling them to learn what typical traffic patterns look like and to flag unusual sequences as potential threats. By capturing the temporal dependencies within the data, LSTMs are more accurate at distinguishing between regular fluctuations and true anomalies, reducing false positives. Additionally, LSTMs are robust against noisy data and can adapt to new patterns of normal behavior, making them valuable for dynamic cybersecurity environments. Overall, the ability of LSTMs to recognize both long- and short-term dependencies makes them a powerful tool for proactive cyber-attack detection and response. The process begins with Log Data Parsing, where the parse_can_log function processes CAN log files to extract crucial elements like timestamps, message IDs, DLC (Data Length Code), and data fields using a regular expression pattern. Any lines that don't match the expected format are logged separately for review, ensuring no data is overlooked. The parsed data is converted into a Pandas DataFrame for further processing. Next, in Data Preparation, the system engineers new features such as Time_Diff (time differences between log entries), ID_Freq (frequency of each message ID), and Data_Byte_Count (the count of data bytes per message). Labels are assigned to the data, marking entries as normal (0) or indicative of a DoS attack (1), based on predefined conditions like ID frequency. During Exploratory Data Analysis, the class distribution of the labels is analyzed to ensure a mix of normal and attack samples, as imbalanced classes could affect model performance. Counts of both normal and attack samples are displayed to validate the dataset's adequacy. The Feature and Target Preparation step isolates key features (Time_Diff, ID_Freq, and Data_Byte_Count) for training, while the target variable (Label) represents the class of each entry. These features are reshaped into 3D arrays to align with the input requirements of LSTM models. In the Data Splitting and Balancing phase, the data is split into training and testing sets. To handle class imbalances, SMOTE (Synthetic Minority Oversampling Technique) is applied to the training data, generating a balanced dataset by synthesizing new samples for the minority class. The Model Definition involves constructing an LSTM-based neural network using TensorFlow's Keras. The model comprises an LSTM layer, a dropout layer to prevent overfitting, and a dense output layer with a sigmoid activation function for binary classification. For Training, the model is trained on the balanced dataset for 10 epochs, with a batch size of 64. This allows the model to learn patterns in the sequential data effectively. In the Evaluation phase, the model's performance is tested on unseen data. Key outputs include a confusion matrix, a classification report detailing precision, recall, and F1 scores, and a precision-recall curve to illustrate the trade-offs between precision and recall at various thresholds.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

National Level Conference – AITCON 2K25

Adarsh Institute of Technology & Research Centre, Vita, Maharashtra

Vol. 12, Special Issue 1, March 2025

Overall model accuracy is also calculated to assess its effectiveness. Finally, the Visualization step includes plotting the precision-recall curve for a comprehensive understanding of the model's performance. This curve helps identify the balance between false positives and false negatives, which is critical in security applications like DoS attack detection.

NLP

NLP can enhance cyber-attack detection in electric vehicles (EVs) by monitoring and analyzing the text-based commands and communications within EV systems. EVs interact with various internal components (like battery management systems and autonomous driving functions) and external entities (such as charging stations and traffic infrastructure) through networked communications. NLP models can scrutinize these communications for irregular patterns, syntax anomalies, or unauthorized command sequences that might indicate a potential cyber threat. For instance, if a charging station sends a message containing unusual or malicious commands to alter charging parameters, NLP algorithms can detect these suspicious patterns by comparing them with known safe command structures. Additionally, NLP models can analyze logs and diagnostic messages to identify discrepancies or unusual language that may signal system tampering, unauthorized access, or compromised components. This application of NLP enhances the EV's ability to identify and mitigate cyber threats in real time, providing a layer of defense against attacks targeting communication protocols or attempting to disrupt critical vehicle functions. To achieve the best performance metrics possible across all levels of the cyber-attack detection system multi-objective optimization which is also referred to as MOO is important. Increasing the detection accuracy is one of the main aims of the system implementation, since it will ensure proper addressing of cybercrimes such as unsuccessful unauthorized accesses or data modification. At the same time, the number of false positives must be minimized, as numerous false alerts can lead to unnecessary interruptions and reduce the reliability of the system. MOO to the advance speed on detection and use of an efficient algorithm. In the context of an electric car, the detection system has to run in real time and has to do so while using the least amount of resources from the vehicle. To facilitate detection with little compromise to the functioning of the vehicle, MOO enhances the balance among high detection accuracy, low rate of false positives and minimum time of processing. Taking in these several aspects helps MOO formulate a robust, efficient and flexible cyber-attack detection framework for EVs. Natural Language Processing (NLP) plays a critical role in improving the analysis of Controller Area Network (CAN) datasets for electric vehicles by allowing deeper insights and actionable outcomes. The datasets usually consist of structured data, such as sensor readings, in addition to unstructured textual information, such as error codes or diagnostic logs. NLP can process and interpret these logs, categorize and structure them to identify patterns, detect anomalies, and correlate error messages with potential root causes. This will allow for efficient diagnostics and predictive maintenance, reducing downtime and improving vehicle reliability. Furthermore, when combined with user feedback or external textual data, NLP can perform sentiment analysis to understand user perceptions of vehicle performance or detect behavioral patterns affecting vehicle operations. NLP is used to bridge structured CAN data and unstructured textual information for more intelligent monitoring, diagnosis, and optimization of EV systems. NLP is an interaction process between computers and human language. This branch of computer science delivers a precise understanding of the data for further analysis. Human languages are broken down into parts to find the grammatical structure and provide the appropriate meaning of the sentence, which is an integral part of the data processing system [14]. When a high amount of data is analyzed, NLP is the best collection of data or method that can minimize latency in a computer. The emerging technology related to EV is offering better types of services and functionality for users via automatic driving skills [15]. This is because, in terms of user safety, EV is ensuring safety from various services that can enhance system feasibility. Hence, EV, using NLP, provides users with an error-free communication procedure that reduces the rate of EV accidents [16]. NLP provides features like text format, text structure, and sentence size that improve the classification and identification rate accuracy. Therefore, NLP determines the format of text and structure to identify the text's actual meaning and content, providing an accurate set of data for the data processing system in EVs. NLP uses a process called "knowledge discovery" that identifies the meaning of the text and improves the feasibility of EVs

Multi objective Jaya Algorithm

$$O_{p+1,q,r} = O_{p,q,r} + \alpha_{p,q,1}\left(O_{p,q,best} - \text{abs}(O_{p,q,r})\right) - \alpha_{p,q,2}\left(O_{p,q,worst} - \text{abs}(O_{p,q,r})\right) \quad (2)$$

Here best and worst represent the index of the best and worst solutions among the population. p, q,r are the index of iteration, variable, and candidate solution. $O_{p,q,r}$ means the q-th variable of r th candidate solution in p-th iteration. $\alpha_{p,q,1}$ and $\alpha_{p,q,2}$ are numbers generated randomly in the range of [0,1].

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

National Level Conference – AITCON 2K25

Adarsh Institute of Technology & Research Centre, Vita, Maharashtra

Vol. 12, Special Issue 1, March 2025

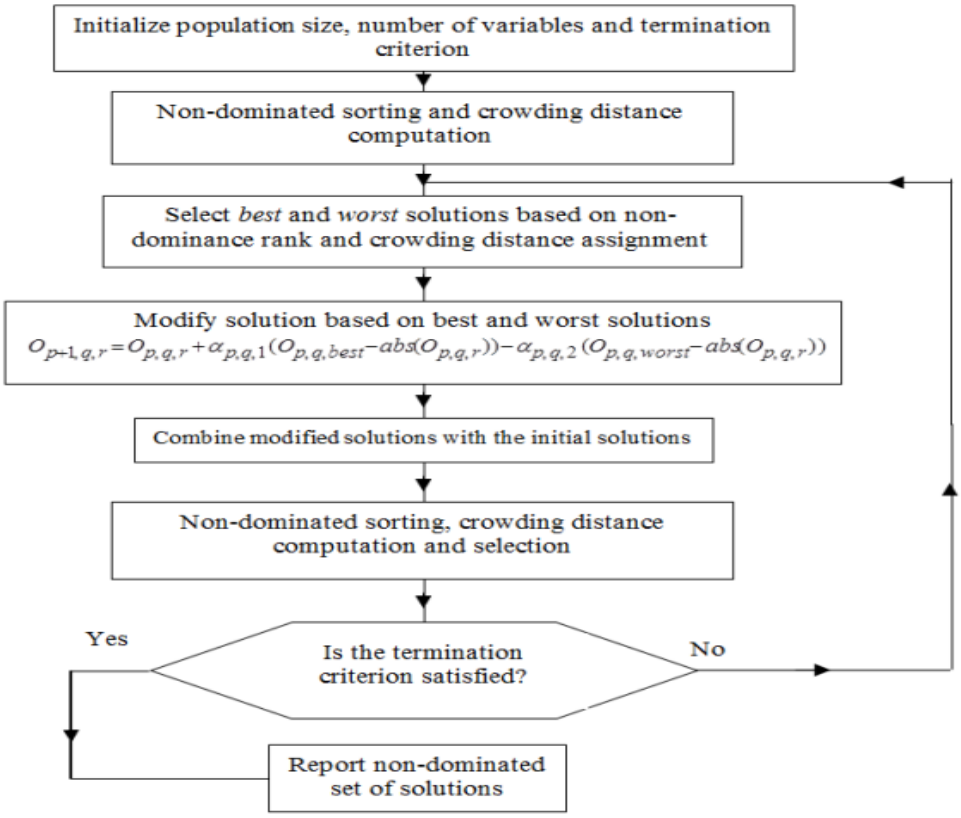


Fig3 Flow Chart of MO Jaya Algorithm [13]

Dataset Used

Dataset Description:

The fig.4 shows the CAN Dataset

Timestamp, CAN ID, DLC, DATA [0], DATA [1], DATA [2], DATA [3], DATA [4], DATA [5], DATA [6], DATA [7]

1. Timestamp: The time when data is recorded.
2. CAN ID: CAN message in HEX format (ex. 043f)
3. DLC: Data bytes from 0 to 8
4. DATA [0~7]: data value (byte)

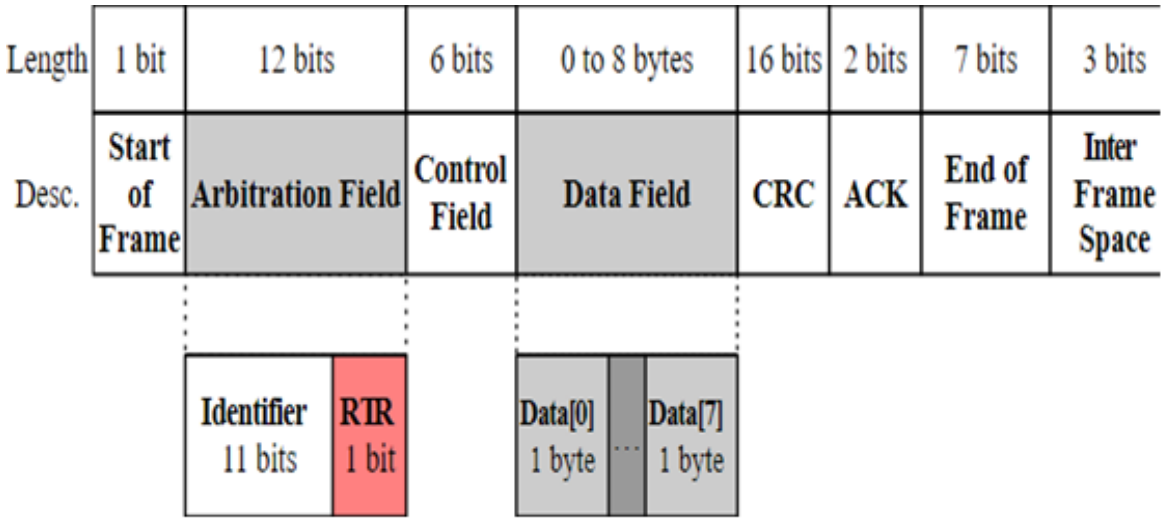


Fig 4. CAN Dataset [12]

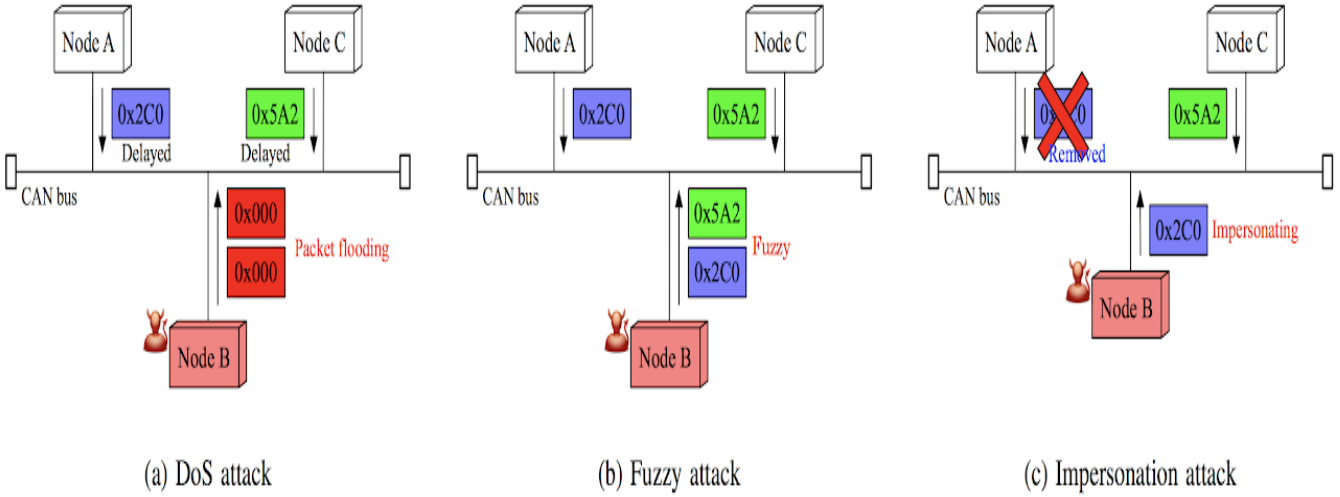
IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

National Level Conference – AITCON 2K25

Adarsh Institute of Technology & Research Centre, Vita, Maharashtra

Vol. 12, Special Issue 1, March 2025



(a) DoS attack (b) Fuzzy attack (c) Impersonation attack

Fig 5. Attack Description [12]

The diagram outlines three types of cyberattacks that can be executed against a Controller Area Network (CAN) bus system implemented in electric vehicles:

Targeting Attacks

DoS Attack: In this case, Node B injects a large volume of packets such as the zero packet 0x000 to the CAN bus and this packet has a high priority which causes transmissions which are intended for Node A or Node C to be delayed.

Fuzzy Attack: In this instance, Node B sends multiple random or disallowed packets, such as 0x5A2 or 0x2C0, into the communication, which subsequently damages the message exchange, and further complicates the communication system.

Impersonation Attack: Messages are sent by Node B to Node A with the intention of impersonating it and in this case, possible disabling of the true communication of Node A happens, such as 0x2C0 e.g. message A.

Relay Attack

The term "relay attack" describes theft using the most common tactic for electric vehicle keyless entry systems: how a hacker intercepts and relays the radio signal from the key fob of a car owner to the vehicle, unlocking and starting up the vehicle without physically possessing the key. In essence, it tricks the car into thinking that the owner is near it by stretching the signal from their key fob using specialized equipment.

Spoofing

A "spoofing attack" in the electric vehicle cybersecurity world occurs when an attacker masquerades as a trusted party to obtain unauthorized access to vehicle systems, commonly by tampering with communication protocols and transmitting malicious data, potentially disrupting critical functions like navigation, braking, or charging, by fooling the vehicle into believing it is receiving data from a trusted source; essentially, it is similar to a case where a person impersonates another to trick the car into performing actions that the car would not normally do.

Firmware Manipulation

Firmware manipulation" in the context of electric vehicles is the act of changing the embedded software code that controls various functions in an electric vehicle, including motor control, battery management, or charging processes that can change a mode of operation and potentially allow unintended access in the case of malfunctions and breaches of security.

V.CONCLUSION

This work gives an overarching system architecture that has been designed for recognition, detection and mitigation of cyberwarfare against EVs by applying MOO techniques along with advanced machine learning approaches. The basic system seams have been enhanced with additional functionalities for data collecting, pre-analysis, data, and machine learning, anomaly detection and reaction, as well as data storage allowing an overall comprehensive solution to EVs' vulnerability against many known and unknown threats. To ensure the effectiveness and reliability of the attack detection system, multi-objective optimization uses the trade-off between different performance measures, such as detection accuracy, false positives and computational cost. In addition, the system does not require extensive training on different attack patterns since it uses a combination of supervised and unsupervised learning algorithms, and further damage is reduced by embedding over-parameterization so that the model easy to monitor and quick to respond. This approach makes it possible to maintain the reliability and security of EVs while increasing the effectiveness of measures to improve the cybersecurity of the automotive industry. All the aspects covered this approach gives a balance between security and usability making it possible to not only protect electric vehicles but restore the security of the existing approaches.

REFERENCES

[1] Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., & Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. In Proceedings of the 20th USENIX Conference on Security (pp. 77-92).

[2] Miller, C., & Valasek, C. (2013). Adventures in automotive networks and control units. In Def Con (pp. 260-264).

[3] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1-58.

[4] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys \& Tutorials, 18(2), 1153-1176.

[5] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In Proceedings of the 2010 IEEE Symposium on Security and Privacy (pp. 305-316).

[6] Gao, Y., Guo, J., Ma, Y., & Zhao, L. (2018). A machine learning-based intrusion detection method for in-vehicle networks. IEEE Access, 6, 60040-60051.

[7] Zhang, Y., Wang, L., Sun, Y., & Zhang, H. (2019). Machine learning-based cyber-attack detection for electric vehicle battery management systems. IEEE Transactions on Industrial Electronics, 66(10), 8896-8906.

[8] Cristianini, N., & Shawe-Taylor, J. (2000). An introduction to support vector machines and other kernel-based learning methods. Cambridge: Cambridge University Press.

[9] Breiman, L. (2001). Random forests. Machine Learning, 45(1), 5-32.

[10] Liu, F. T., Ting, K. M., & Zhou, Z. (2008). Isolation forest. In Proceedings of the 2008 Eighth IEEE International Conference on Data Mining (pp. 413-422).

[11] Hinton, G. E., & Salakhutdinov, R. R. (2006). Reducing the dimensionality of data with neural networks. Science, 313(5786), 504-507.

[12] https://ocslab.hksecurity.net/Dataset/CAN-intrusion-dataset

[13] Rao, R. V., Rai, D. P., Ramkumar, J., & Balic, J. (2016). A new multi-objective Jaya algorithm for optimization of modern machining processes. Advances in Production Engineering & Management, 11(4).

[14] Putri, T.D. Intelligent transportation systems (ITS): A systematic review using a Natural Language Processing (NLP) approach. Heliyon 2021, 7, e08615.

[15] Huang, D.J.; Lin, H.X. Research on Vehicle Service Simulation Dispatching Telephone System Based on Natural Language Processing. Procedia Comput. Sci. 2020, 166, 344–349. [CrossRef]

[16] Runck, B.C.; Manson, S.; Shook, E.; Gini, M.; Jordan, N. Using word embeddings to generate data-driven human agent decisionmaking from natural language. GeoInformatica 2019, 23, 221–242. [CrossRef]

.