Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, No.2, December : 2024

CYBER ATTACK DETECTION FRAMEWORK FOR SECURING ELECTRIC VEHICLES

Mr. Rahul Dilip Dhongade, K J College of Engineering research and Management, Dept. of CO Pune University
Dr. Nikita Kulkarni K J College of Engineering research and Management, Dept. of CO Pune University

ABSTRACT
With the arrival of electric vehicles (EVs), which offer a sustainable alternative to conventional internal combustion engine vehicles, the automobile industry has experienced a significant upheaval. EVs are more susceptible to hacking, though, since they are more heavily connected with digital technologies. These attacks put EV owners and their cars at serious danger by undermining the EVs' dependability, efficiency, and safety. The use of machine learning techniques to detect and lessen cyberattacks on electric vehicles is examined in this article. the combination of supervised machine learning algorithms like Random Forest and Support Vector Machine (SVM) with unsupervised methods like autoencoders and isolation forests. The plan is to collect and analyze a large amount of data from various EV components, control units, and communication networks. Using the benefits of each technique, the multi-layer detection framework increases the reliability and accuracy of cyber attack detection. The supervised algorithms are trained on labeled datasets to classify current types of cyber-attacks, while the unsupervised algorithms use anomaly detection to find new or emerging threats. An actual dataset is used to evaluate the performance of the proposed model. This study highlights how crucial machine learning is to ensuring the safe and dependable operation of the next generation of electric cars and shielding them from fresh cyberattacks.

Keywords—
electric vehicles, machine learning, artificial intelligence, cybersecurity, authentication, and protection.

I. Introduction
Modern digital technology is integrated into electric vehicles (EVs) to enhance performance, connectivity, and user experience. EVs represent a major advancement toward sustainable and environmentally friendly transportation. Because of the increasing integration of smart software systems and Internet of Things (IoT) components, EVs are becoming more and more susceptible to various cyber assaults. Cyberattacks that target electric vehicles have the potential to cause major problems, including changing the vehicle's controls, obtaining private data, harming the infrastructure that supports charging, and putting the passengers' safety in jeopardy. Hackers find EVs to be attractive targets since they are networked and rely on communication networks for several functions, such as remote diagnostics, navigation, and battery management. The unique vulnerabilities of electric vehicle (EV) systems often call for novel solutions, as standard cybersecurity measures are often not adequate to address the unique issues raised by the automotive sector.
In this context, machine learning (ML) offers a practical way to enhance the detection and prevention against cyberattacks directed at electric vehicles. ML algorithms can analyze vast volumes of data generated by EV components in real-time, allowing for the detection of trends and aberrations that may indicate a potential cyberthreat. Two of machine learning's numerous advantages are its ability to learn from historical data and adapt to new attack types, making it a useful tool for building robust cybersecurity frameworks.
This study looks into potential applications of machine learning techniques for the detection of cyberattacks on electric vehicles. We focus on a combination of supervised learning methods, such as Random Forest and Support Vector Machines (SVM), and unsupervised learning algorithms, such as Isolation Forest and Autoencoders, to build a comprehensive detection framework. Our approach involves collecting and analyzing data from several EV subsystems, including control units,

communication networks, and battery management systems, to identify potential security vulnerabilities.

The remaining portions of the text are arranged as follows: In Section 2, the work on machine learning for cybersecurity and anomaly detection for electric vehicles is reviewed. Section 3 provides a detailed description of the recommended methodology, which includes feature extraction, data collection, and the creation of machine learning algorithms. Results of our examinations and evaluations are displayed in Section 4. The implications of our research are outlined in Section 5, along with suggestions for future directions. Our research aims to support the development of cybersecurity strategies that will safeguard electric vehicles and ensure their dependable and safe operation in an increasingly connected environment.

II. Literature Review

Electric vehicles (EVs) are more frequently the subject of cyberattacks that compromise their security and functionality. Checkoway et al. [1] shown how internal car systems might be remotely exploited through interfaces like Bluetooth and cellular networks. Miller and Valasek [2] brought attention to important safety concerns and further illustrated the potential for remote control vehicle operations. In order to protect EVs, our findings emphasize how crucial it is to have robust cybersecurity defenses against a variety of attack vectors, such as internal systems, communication networks, and charging infrastructure. Anomaly detection, which focuses on identifying deviations from the norm that may point to a security concern, is a crucial cybersecurity tactic. Chandola and collaborators. provided a comprehensive examination of anomaly detection techniques, emphasizing their application in a range of domains, including network security. Despite their widespread use, statistical and rule-based approaches usually fail to keep up with the evolving nature of cyber threats, necessitating the deployment of more dynamic solutions like machine learning. The application of machine learning (ML) has become essential for strengthening cybersecurity defenses. Buczak and Guven [4] noted in their evaluation of the application of machine learning (ML) for network intrusion detection that algorithms such as Support Vector Machines (SVM) and Random Forests are effective in classifying hostile activities. Sommer and Paxson [5] stressed the need for continual modification and learning from new data in their assessment of the advantages and challenges of applying machine learning (ML) in network intrusion detection systems. Many studies have focused in particular on machine learning applications for EV cybersecurity. Gao et al. [6] introduced a machine learning-based intrusion detection system for connected and autonomous cars that can identify irregularities in vehicle communication data. This system employs deep learning methods. Zhang et al. aimed to improve the accuracy of cyberattack detection on EV battery management systems developed a machine learning framework that makes use of both supervised and unsupervised learning techniques. Supervised learning methods such as Random Forest and Support Vector Machines (SVM) are widely used in cybersecurity to identify anomalies. Cristianini and Shawe-Taylor [8] claim that because SVM is effective at binary classification tasks, it can be used to distinguish between benign and malignant activity. Breiman [9] introduced Random Forest, a technique that reduces overfitting and improves detection performance by combining the output of many decision trees. These algorithms have shown tremendous promise in identifying and classifying cyberthreats across a wide range of domains.

Unsupervised learning algorithms like isolation forests and autoencoders are crucial for finding novel or unidentified attacks. As demonstrated by Liu et al. [10], Isolation Forest isolates data in the feature space, which makes it helpful for identifying abnormalities. Autoencoders are a type of neural network that may be used to learn representations of data and employ input reconstruction to discover irregularities. Hinton and Salakhutdinov [11] discussed this technique. These algorithms are particularly helpful since they can identify underlying patterns and deviations without the requirement for labeled data. EV cybersecurity still faces a number of problems despite significant advances.

Cyber dangers are complex and dynamic; therefore, detection strategies need to be modified often. Additionally, integrating heterogeneous data streams from various EV components significantly impedes real-time processing and data standardization.

Future research should focus on developing more adaptable and comprehensive machine learning models, improving data integration techniques, and enhancing real-time threat detection capabilities in order to ensure the robust cybersecurity of electric cars.

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,	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

Paxson and Sommer [5]					
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 detects and stops cyberattacks on electric vehicles (EVs) by utilizing machine learning techniques and an advanced architecture. The design is composed of several interconnected modules, each of which performs a specific function to ensure the overall security of the EV. Unprocessed data is gathered by the data collection system from a variety of sources, including network traffic, actuators, and sensors on the EV. Sensors and actuators monitor the car's internal systems, such as the battery management system, vehicle control systems, and communication interfaces.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, No.2, December : 2024

Network traffic data is also collected in order to monitor communications between the EV and external entities such as infrastructure, other vehicles, and charging stations. This kind of data collection is necessary to detect any anomalous activity or potential cyberthreats. To ensure coherence, the data needs to be cleansed by eliminating extraneous information and noise, standardizing it, and determining relevant attributes for the machine learning models. Appropriate pretreatment is required for a more accurate and effective analysis later on. Machine learning, the core of the system, uses both supervised and unsupervised learning methods. Support Vector Machines (SVM) and Random Forest, two supervised learning algorithms, are used to identify known types of cyberattacks by classifying data based on predefined patterns. Unsupervised learning methods such as Autoencoders and Isolation Forest are used to detect novel or unidentified attacks by looking for abnormalities in the data that deviate from expected behavior. This combination of techniques ensures strong detection capabilities by addressing both emerging and known threats. The anomaly continuously monitors real-time data from the EV. It generates alerts for critical threats and assigns a severity rating to anomalies based on their potential consequences. This real-time scoring and monitoring system lowers the likelihood that the car and its systems may be harmed by enabling quick identification and response to cyberattacks. The takes prompt action to lessen known cyberthreats. These actions could include limiting the car's functionality, isolating affected parts, or turning off particular systems in order to prevent further harm. Additionally, this module keeps track of all abnormalities discovered and actions taken for further research and reporting, which contributes to the continuous enhancement of the system's security measures.

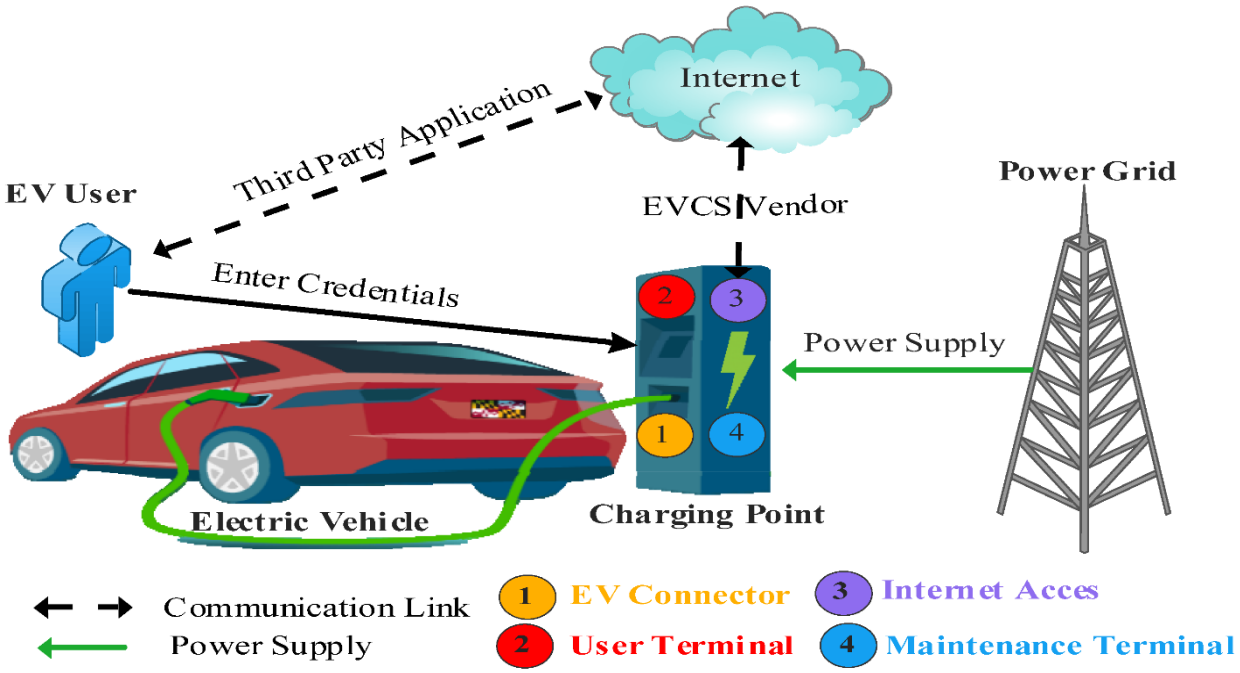

Figure1.EVCSs with Vulnerable points.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, No.2, December : 2024

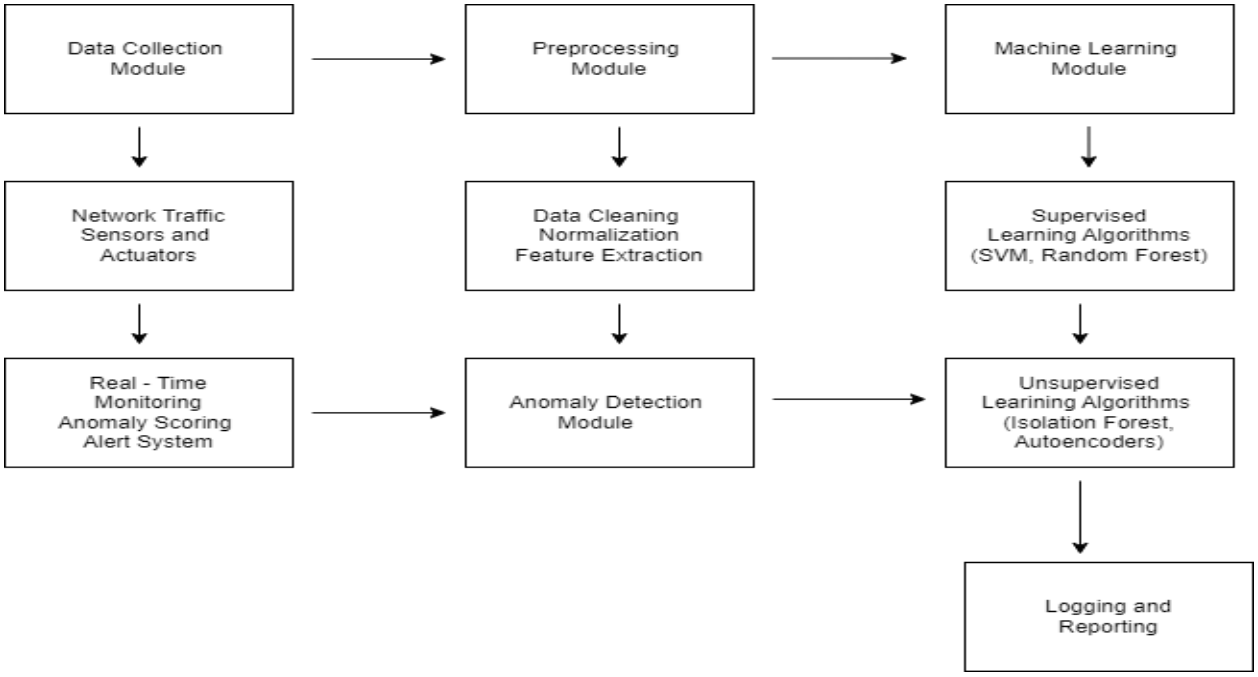

Figure 2. Proposed System Work Flow

3.1 Preprocessing

Data Cleaning: This sub-module removes noise and irrelevant information from the collected data to improve the analysis's accuracy.

Normalization: This sub-module normalizes data to ensure consistency across several sources in preparation for machine learning models.

Feature Extraction: The relevant features that machine learning models will use to detect abnormalities are gathered in this sub-module.

Supervised Learning Algorithms: This sub-module detects known types of cyberattacks by classifying data based on pre-established patterns using algorithms such as Random Forest and Support Vector Machines (SVM).

Unsupervised Learning Algorithms: In order to uncover new or undiscovered attacks, this sub-module looks for anomalies in the data that deviate from usual behavior using techniques like autoencoders and isolation forests. This combination ensures robust detection capabilities that cover both emerging and known threats.

IV. Conclusion

This paper provides a robust system architecture to detect and mitigate cyberattacks on electric vehicles (EVs) using state-of-the-art machine learning techniques. The proposed system combines modules for data collection, preprocessing, machine learning, anomaly detection, reaction, and data storage to offer an all-encompassing approach to safeguarding EVs against known and undiscovered threats. The system's combination of supervised and unsupervised learning algorithms ensures effective cyberattack detection, while real-time monitoring and quick response measures help minimize potential damage. This design increases the security of EVs while also assisting the automotive industry in its ongoing development and improvement of cybersecurity protections. All things considered, the proposed strategy is a significant advance over existing techniques for protecting electric vehicles from cyberattacks, guaranteeing the stability and security of these extensively utilized technology.

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.